

DEPARTMENT OF DEFENSE
PUBLICATION SYSTEM

CHANGE TRANSMITTAL

DoD 5200.2-R

OFFICE OF THE SECRETARY OF DEFENSE
Assistant Secretary of Defense for
Command, Control, Communications, and Intelligence

CHANGE ³
February 23, 1996

PERSONNEL SECURITY PROGRAM REGULATION

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, has authorized the following pen and page changes to DoD 5200.2-R, "Personnel Security Program Regulation," January 1987:

PEN CHANGES

Page iv, Chapter II, Section 5, page numbers for 2-500 and 2-501. Change "II-9" to "11-10"

Page v, Chapter III, Section 4.

Delete "3-402 Naturalized United States Citizens . . . 111-8"

Re-number the index listing "3-403 through 3-408" to "3-402 through 3-407"

Re-number page references as follows:

"III-8" to "III-7"

"III-9" to "III-11"

"III- 10" to "III-11"

"III-1 1" to "111-12"

"HI-13" to "III-14"

Section 5, page numbers for 3-502 and 3-503. Change "111-14" to "111-15"

Section 6, page number for 3-612. Change "III-21" to "III-20"

Page vi

Chapter III, Section 7

Page numbers for 3-706 and 3-707. Change "III-23" to "III-22"

Page numbers for 3-709 and 3-710. Change "III-24" to "HI-23"

Section 8, page number for 3-800. Change "III-24" to "III-23"

Page vii

Chapter VII, page number for 7-103. Change "VII-2" to "WI-3"

Chapter VIII

Section 2, page number for 8-200. Change "VIII-2" to "VIII-3"

Change index listing for "8-202" to "8-203" and page number "VIII-4" to "VIII-5"

Insert new index listing "8-202 Due Process Review . . . VIII-5"

Section 3, page numbers for 8-300 and 8-301. Change "VIII-4" to "VIII-5"

NUMBER	DATE	DEPARTMENT OF DEFENSE PUBLICATIONS SYSTEMS TRANSMITTAL
5200. 2-R, Change 3	February 23, 1996	

INSTRUCTIONS FOR RECIPIENTS (continued)

Page I-1, Chapter I, Section 1,

Reference (a), lines 1 through 3. **Change** to read "DoD 5200.2-R, 'Personnel Security Program,' January 1987, authorized by DoD Directive 5200.2, May 6, 1992"

Reference (c), line 2. Change "August 12,1985" to "February 2,1992"

PAGE CHANGES

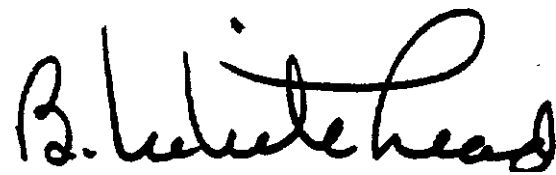
Remove: Pages viii, II-7 through II-1 1, III-7 through III-24, IV-1 & IV-2, VII-1 through VII-3, VIII-1 through Viii-4, A-1 **through** B-12, F-1 & F-2, and I-1 **through** I-27

Insert: Attached replacement pages and new pages VIII-5, XII-1 through XII-4, F-3, L-1 through L-1 8, M-1, and N-1

Changes appear on pages viii& **ix**, H-7 through II-9, III-7 through III-11, III-13& III-14, III-17, IV-1 & IV-2, VII-2, VIII-1 through VIII-5, A-1 & A-2, B-1 through B-10, F-1 through F-3, and 1-1 through 1-17 and are indicated by marginal bars.

EFFECTIVE DATE

The above change are effectively immediately.



B.C. WHITEHEAD "
Director
Correspondence and Directives

Attachment
87 pages

9-101 Management Responsibility	IX-1
9-102 Supervisory Responsibility	IX-1
9-103 Individual Responsibility	Ix-2
9-104 Co-worker Responsibility	IX-3

Section 2

SECURITY EDUCATION

9-200 General	IX-3
9-201 Initial Briefing	IX-3
9-202 Refresher Briefing	IX-4
9-203 Foreign Travel Briefing	IX-4
9-204 Termination Briefing	Ix-5

CHAPTER X

SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

10-100 General	X-1
10-101 Responsibilities	x-1
10-102 Access Restrictions	X-1
10-103 Safeguarding Procedures	x-2
10-104 Records Disposition	x-2
10-105 Foreign Source Information	X-3

CHAPTER XI

PROGRAM MANAGEMENT

11-100 General	XI-1
11-101 ResponsibilitiesXI-1
11-102 Reporting RequirementsXI-2
11-103 InspectionsXI-2

CHAPTER XII (New)

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX

12- 00	Genera	XII- 1
12-101	AccessXII-1
12-102	Investigative DataXII-2
12-103	Adjudicative DataXII-2
12-104	Notification to Other ContributorsXII-3
12-105	Security Requirements for the DCIIXII-3
12-106	Disclosure InformationXII-3

APPENDICES

Appendix A -	References (continued)	A-1	
Appendix B -	Investigative Scope	B-1	
Appendix C -	Request Procedures	C-1	
Appendix D -	Tables for Requesting Investigations	D-1	
Appendix E -	Reporting of Non derogatory Cases	E-1	
I Appendix F -	DoD Security Clearance and/or SCI Access Determination Authorities	F-1	I
Appendix G -	Guidelines for Conducting Prenomination Personal Interviews	G-1	
Appendix H -	(left blank for future use)		
Appendix I -	Adjudicative Guidelines for Determining Eligibility for Access to Classified Information	I-1	
Appendix J -	Overseas Investigations	J-1	
Appendix K -	ADP Position Categories and Criteria for Designating Positions	K-1	
Appendix L -	Sample Notifications for Adverse Personnel Security Determinations	L-1	
Appendix M -	Structure and Functioning of the Personnel Security Appeal Board	M-1	
Appendix N -	Conduct of a Personal Appearance Before an Administrative Judge (AJ)	N-1	

Section 4

AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

2-400 **General**

The DIS provides a single centrally directed personnel security investigative service to conduct **personnel** security investigations within the 50 states, District of **Columbia**, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23 (reference (n)). DIS will request the Military Departments or other appropriate Federal Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Assistant Secretary of Defense (Intelligence and Security). In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

2-401 **Subversive Affiliation**

a. **General.** In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. **Specifically**, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

- (1) Overthrowing the Government of the United States or the government of a state;
- (2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions:
 - (a) The **functions** of the Government of the United States, or
 - (b) The **functions** of the government of a state;
- (3) Depriving persons of their civil rights under the Constitution or laws of the United States.

b. **Military Department/FBI Jurisdiction.** Allegations of activities covered by criteria a. through f. of paragraph 2-200 of this Regulation are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI (reference (o)). Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a **personnel** security investigation conducted by DIS, they **shall** be referred immediately to either the FBI or to a military department counterintelligence agency as appropriate.

c. **DIS Jurisdiction.** Allegations of activities limited to those set forth in criterion g. through q. of paragraph 2-200 of this Regulation shall be investigated by DIS.

2-402 Suitability Information

a. **General.** Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by criteria g. through q. of paragraph 2-200 of this Regulation. Almost all unfavorable **personnel** security determinations made by DoD authorities are based on **derogatory** suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal **from** Federal employment under OPM regulations.

b. **Pre-clearance Investigation.** Derogatory suitability information, except that covered in d. below, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel **security** clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria g. through q. of paragraph 2-200.

c. **Postadjudicative Investigation.** Derogatory suitability allegations, except those covered by d. below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified **information**, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior **shall** also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph 3-701 applies. Postadjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations lie outside the DoD personnel security program and are not a proper investigative **function** for departmental counterintelligence organizations, Component **personnel** security authorities, or **DIS**.

d. **Allegations of Criminal Activity.** Allegations of possible criminal conduct arising during a personnel security investigation shall be referred to the appropriate Department of Defense criminal investigative agency, Military Department or civilian jurisdiction unless the limitations in paragraph 2-402d(1) through 2-402d(3) below, apply. Where the allegation concerns a potential violation of the Uniform **Code** of Military Justice, Military Department investigative Agencies have primary investigative jurisdiction. The following limitations apply to referrals to all law enforcement agencies, both military and civilian.

(1) Allegations shall not be referred or reported to law enforcement agencies where agreements with the agency or in cases where there is no **agreement**, past experience indicates that the jurisdiction does not have a substantial interest in prosecution of the offense or in receiving reports of the offense either due to the type or offense involved or the circumstances under which it occurred.

(2) Allegations about private **consensual** sexual acts with adults shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. That limitation does not apply to allegations that an individual attempted, solicited, or committed a criminal offense in the following circumstances:

(a) **By** using force, coercion, or intimidation.

- (b) With a person under 17 years of age.
- (c) Openly in public view.
- (d) For compensation or with an offer of compensation to another individual.
- (e) While on active duty in, or on duty **in** a Reserve component of, the Armed Forces of the United States and

- 1 Aboard a military vessel or **aircraft**; or
 - 2 With a subordinate in circumstances that violate customary military superior-subordinate relationships.

Exceptions to that limitation will be made only with the specific written authorization of the General Counsel of the Department of Defense, or his or her designee.

(3) Information about an individual's sexual orientation or statements by **an** individual that he or she is a homosexual or **bisexual**, or words to that **effect**, shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. If investigative reports containing such information are referred to law enforcement agencies or **Military** Departments for other reasons, information subject to the limitations in this paragraph will be removed.

2-403 Hostage Situations

a. **General.** A hostage situation exists when a member of subject's immediate family or such other person to whom the individual is bound by obligation or **affection** resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this **category** of investigation is based on the possibility that an individual in such a situation might be **coerced**, influenced, or pressured to act contrary to the interests of national security.

b. **DIS Jurisdiction.** In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by **DIS**.

c. **Military Department and/or FBI Jurisdiction.** Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned-or should there exist any other evidence that the individual is actually being **coerced**, **influenced**, or pressured by an element inimical to the interests of national security-then the case becomes a counterintelligence matter (outside of investigative jurisdiction of **DIS**) to be referred to the appropriate military department or the FBI for investigation.

2-404 Overseas Personnel Security Investigations

Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate military department investigative organization. Only **postadjudication** investigations involving an overseas subject may be referred by the requester **directly** to the military department investigative organization having investigative responsibility in the overseas area concerned (see Appendix J) with a copy of the investigative request sent to DIS. In such cases, the military department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

Section 5

LIMITATIONS AND RESTRICTIONS

2-500 Authorized Requesters and Personnel Security Determination Authorities

Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in paragraph 5-101 and Appendix F.

2-501 Limit Investigations and Access

The number of persons cleared for access to classified information **shall** be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for personnel security investigations.

2-502 Collection of Investigative Data

To the greatest extent practicable, personal information relevant to personnel **security** determinations shall be obtained directly from the subject of a personnel security investigation. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate **from** knowledgeable personal sources, particularly subject's peers, and through checks of relevant records including school, **employment, credit**, medical, and law enforcement records.

2-503 Privacy Act Notification

Whenever personal information is solicited from an individual **preparatory to the initiation** of a personnel security investigation, the individual must be informed of (1) the authority (statute or Executive order that authorized solicitation); (2) the principal purpose or purposes for which the information is to be used; (3) the routine uses to be made of the information, (4) whether furnishing such information is mandatory or voluntary (5) the effect on the individual, if any, of not providing the information and (6) that subsequent use of the data maybe employed as part of an aperiodic, random process to screen and evaluate continued eligibility for access to classified information.

2-504 Restrictions on Investigators

Investigations shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health should be avoided unless the question is relevant to the criteria of paragraph 2-200 of this Regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this Regulation, investigators shall:

- a. Investigate only cases or persons assigned within their **official** duties.
- b. Interview sources only where the interview can take place in reasonably private surroundings.

c. Always present credentials and inform sources of the reasons for the investigation.. Inform sources of the subject's accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of **personnel** security investigations are outlined in paragraph 2-503.

d. Furnish only necessary identity data to a source, and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

e. Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretap, or eavesdropping devices.

f. Refrain **from** accepting any case in which the investigator knows of circumstances that might adversely affect his fairness, impartiality, or objectivity.

g. **Refrain**, under any circumstances, from conducting physical searches of subject or his property.

h. Refrain **from** attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DoD medical authorities. However, review and collection of medical record information maybe accomplished by authorized investigative personnel.

2-505 **Polygraph** Restrictions

The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48, (reference (p)).

(b) **NACI**: Civilian employees

(c) **ENTNAC**: First-term **enlistees**

(2) Interim Clearance

(a) When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs (b) through (e) below, have been complied with.

(b) Favorable review of DD Form 398-2/SF-85/SF-171 /**DD** Form 48.

(c) **NACI**, **DNACI**, or **ENTNAC** initiated.

(d) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(e) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

c. Confidential

(1) Final Clearance:

(a) **NAC** or **ENTNAC**: Military and contractor employees (except for Philippine national members of the United States Navy on whom a **BI** shall be favorably completed.)

(b) **NACI**: Civilian employees (except for summer hires who maybe granted a final clearance on the basis of a **NAC**).

(2) Interim Clearance

(a) Favorable review of DD Form 398-2/SF 85/SF 17 1/**DD** Form 48.

(b) **NAC**, **ENTNAC** or **NACI** initiated.

(c) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(d) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

d. Validity of Previously Granted Clearances:

Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is **required**, investigative requirements of this directive will be followed.

3-402 Access to Classified Information by Non-U.S. Citizens

a. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a "Limited Access Authorization" (**LAA**) in those rare circumstances where anon-U. S. citizen possesses a unique or unusual skill or expertise that is urgently needed in pursuit of a specific DoD requirement involving access to specified classified information for which a cleared or clearable U.S. citizen is not available.

b. Limitations

(1) LAAs shall be limited only to individuals who have a special skill or technical expertise essential to the fulfillment of a DoD requirement that cannot reasonably be filled by a U.S. citizen.

(2) **LAAs** shall not be granted to personnel who perform routine **administrative** or other support duties, such as secretaries, clerks, **drivers, or** mechanics, unless it has been clearly established that those duties cannot be performed by a U.S. citizen.

(3) Personnel granted LAAs **shall** not be permitted **uncontrolled** access to areas where classified information is stored or discussed. Classified information shall be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

(4) LAA **personnel** shall not be designated as a courier or escort for classified material outside the location in which access is permitted unless they are accompanied by an appropriately cleared U.S. person.

c. Authorized Access Levels

(1) LAAs may be granted only at the SECRET and CONFIDENTIAL level. LAAs for TOP SECRET are prohibited. Interim access is not authorized pending approval of a LAA.

(2) The information the **non-U.S.** citizen may have access to must be approved for release to the person's country or countries of citizenship, in accordance with DoD Directive 5230.11 (reference (11)).

(3) Access to classified information shall be limited or related to a specific program or **project**; the LAA shall be canceled or rejustified as described herein upon completion of the program or project.

(4) Access to classified information outside the scope of the approved LAA shall be considered a compromise of classified information and shall be **investigated**, in accordance with DoD 5200. 1-R (reference (q)).

d. Requirements

(1) The LAA granting authority (Appendix F) may consider issuing an LAA only after a written determination is made that access is essential for a critical mission and no U.S. citizen is available to perform the duties.

(2) When a **non-U.S.** citizen who is nominated for an **LAA** is a citizen of a country with which the United States has an agreement providing for security assurances based on that country's investigative requirements, which are commensurate with the standards provided herein, an LAA may be issued at the requisite level.

(3) In addition to the above, a favorably completed (within the last 5 years) and adjudicated SSBI is required prior to granting an LAA. If the SSBI cannot provide **full** investigative coverage, a polygraph examination (if there are no host country legal prohibitions) to resolve the remaining personnel security issues (See DoD Directive 5210.48 (reference (p))), must be favorably completed before granting access.

(4) If geographical, political or medical situations prevent the **full** completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, a LAA may be granted only with approval of the **ASD(C3I)**.

(5) If an LAA is withdrawn and the individual subsequently is considered for an LAA, the provisions of this paragraph shall apply concerning an **SSBI** and polygraph examination. The scope of the SSBI normally shall cover the period since the previous background investigation or 10 years, whichever is shorter.

(6) A PR shall be conducted on every individual with a **LAA** 5 years from the date of the last PR or SSBI, as appropriate.

(7) All requests for initial LAAs shall contain a detailed justification and plan describing the following

(a) The location of the classified material (security containers) in relationship to the location of the foreign national.

(b) The compelling reason for not employing a cleared or clearable U.S. citizen.

(c) A synopsis of an annual continuing assessment program to evaluate the individual's continued trustworthiness and eligibility for access.

(d) A plan to control access to secure areas and to classified and controlled unclassified information.

e. **LAA Determination Authority**

(1) **LAA** determinations may only be made by an official listed in paragraph B, Appendix F. The designated single authorizing official for the Military Departments, the Unified Combatant Commands, and the DIS precludes an LAA determination by any other **official** at the major command level, or equivalent.

(2) LAA determinations for employees of the Military Departments shall be the sole authority of the Secretary of the Military Department or a single designee such as the Service central **adjudication** facility. Field elements must submit their recommendations for access to the designated official for approval, along with **affiliated** information in support of the action.

(3) The Commander of a Unified Combatant **Command**, or single designee (flag officer or civilian **equivalent**) responsible for implementation of the personnel security program, shall be authorized to issue, deny, or revoke an LAA. LAA determinations by the Unified Combatant Commands shall be reported to the central adjudicative facility of the Military Department in accordance with the assigned **responsibilities** in DoD Directive 5100.3 (reference (mm)) for inclusion in the **DCII**.

(4) All LAA determinations, favorable and unfavorable, shall be entered into the **DCII**.

(5) The administrative action procedures in Chapter 8 do not apply to LAA determinations.

f. **Record**

(1) The LAA granting **authority** shall ensure that a record is created on issuance and maintained for 5 years from the date the LAA ceases. The record shall include the following:

(a) The identity of the individual granted the LAA, to include the **full** name, date and place of birth, current citizenship(s), any SSN, and any national identifying number issued by the individual's country or countries of citizenship;

(b) The individual's status as an immigrant alien or foreign national; if an immigrant alien, the date and place such status was **granted**;

(c) The classification level of the LAA; i.e., SECRET or CONFIDENTIAL;

(d) Date and type of most recent background investigation or PR and the investigating Agency.

(e) Whether a polygraph examination was **conducted**; if so, the date and administering Agency for the most recent examination.

(f) The nature and identity of the classified program materials to which access is authorized and the precise duties performed.

(g) **The compelling** reasons for granting access to the information.

(2) All LAA **SSBIs** and **PRs** shall be conducted under the auspices of the DIS and shall comply with the requirements of Appendix B. The DIS shall initiate leads to the respective Military Department investigative agencies overseas as **well** as the Department of State (DOS). The results of all investigations, to include those conducted by the DOS, shall be returned to the DIS for review and entry into the **DCII** and return to the designated granting official for adjudication. (To expedite matters, the investigation may be initiated locally provided the necessary paperwork has been submitted to the DIS for assignment of a case control number and initiation of such other checks as needed.)

(3) The Unified Combatant Commands shall report LAAs they issue to the applicable DoD Component CAP for entry into the **DCII**. The Unified Combatant Commands shall ensure that all investigative paperwork for the initiation of the SSBI or PR is submitted to the DIS through the designated **single-approval** authority responsible for adjudication and issuance of the LAA.

(4) All LAA nominees must agree to undergo a polygraph examination at any time during the period the LAA is in **effect**, if there is no how-country legal prohibition.

g. All **LAAs** shall be reviewed annually by the issuing component to determine if continued access is in compliance with DoD policy. A report on all **LAAs** in **effect**, including the data required in paragraph 3-402.f.(1) shall be furnished to the **DASD(I&S)** within 60 days after the end of each fiscal year (see subsection 11-102 below).

3-403 Access by Persons Outside the Executive Branch

a. Access to classified information by persons outside the Executive Branch shall be accomplished in accordance with Chapter VII, DoD 5200. 1-R (reference (q)). The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

b. Members of the U.S. Senate and House of Representative do not require **personnel security** clearances. They may be granted access to DoD classified information which relates to matters under the jurisdiction of the respective Committees to which they are assigned and is needed to perform their duties in connection with such assignments.

c. Congressional staff members requiring access to DoD classified information shall be processed for a security clearance **in** accordance with DoD Directive 5142.1 (reference (00)) and the provisions of this Regulation. The Director, Washington Headquarters Services (WI-IS) will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and **grant**, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

d. State governors do not require personnel security clearances. They maybe granted access to specifically designated classified information, on a "need-to-know" basis, based upon affirmation by the Secretary of Defense or the head of a DoD Component or single designee, that access, under **the** circumstances, serves the national interest. Staff personnel of a governor's **office** requiring access to classified information shall be investigated and cleared in accordance with the prescribed procedures of this Regulation when the head of a DoD **Component**, or single designee, affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a "need-to-know" basis.

e. Members of the U.S. Supreme **Court**, the Federal judiciary and the Supreme Courts of the individual states do not require personnel security clearances. They maybe granted access to DoD classified information to the extent **necessary** to adjudicate cases being heard before these individual courts.

f. Attorneys representing DoD military, civilian or contractor **personnel**, requiring access to **DoD** classified information to properly represent their clients, shall **normally** be investigated by DIS and cleared **in** accordance with the prescribed procedures in paragraph 3-401. This shall be done upon certification of the General Counsel of the DoD Component involved in the litigation that access to specified classified **information**, on the part of the attorney **concerned**, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph 3-401, access may be granted with the written approval of an authority designated in Appendix F provided that as a minimum (a) a favorable name check of the FBI **and** the **DCII** has been **completed**, and (b) a DoD Non-Disclosure Agreement has been executed. In post-indictment cases, after a judge has invoked the security procedures of the Classified Information Procedures Act (**CIPA**) (reference (m)), the Department of Justice may elect to conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DoD component

3-404 Restrictions on Issuance of Personnel Security Clearances

Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements. .

Personnel security clearances shall normally not be issued

- a. To persons in nonsensitive positions.
- b. To persons whose regular duties do not require authorized access to classified information.
- c. For ease of movement of persons within a restricted, **controlled**, or industrial **area**, whose duties do not require access to classified **information**.
- d. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service **personnel**, **firemen**, doctors, nurses, police, ambulance drivers, or similar personnel.
- e. To persons working in shipyards whose duties do not require access to classified information.
- f. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.
- g. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.
- h. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.
- i. To persons who perform maintenance on office **equipment**, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.
- j. To perimeter security personnel who have no access to classified information.
- k. To drivers, chauffeurs and food service personnel.

3-405 Dual Citizenship

Persons claiming both U.S. and foreign citizenship shall be processed under paragraph 3-401, above, and adjudicated in accordance with the "Foreign Preference" standard in Appendix I.

3-406 One-Time Access

Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD **personnel** to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such **situations**, and only for compelling reasons in furtherance of the DoD mission, an authority **referred** to in subparagraph **a.**, below, may **grant higher** level access on a temporary basis subject to the terms and conditions **prescribed** below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate **security oversight**. These procedures do not apply when **circumstances** exist which would permit the routine processing of an individual for the higher level clearance. Procedures **and** conditions for effecting emergency one-time access to the next higher classification level areas follows

a. Authorization for such one-time access shall be granted by a flag **o****general** officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security **officials**.

b. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

c. Such access, **once granted**, shall be canceled promptly when no longer **required**, at the conclusion of the authorized period of access, or upon notification from the granting **authority**.

d. The **employee** to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

e. Pertinent local records **concerning** the employee concerned shall be reviewed with favorable results.

f. Whenever possible, access shall be confined to a single instance or at **most**, a few occasions. The **approval** for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of **30** days, written approval of the granting authority is required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been **approved**, such access **shall** be canceled at or before 90 days **from** original date of access.

g. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible **for**: (1) recording the higher-level information actually **revealed**, (2) the date(s) such access is **afforded**, and (3) the daily retrieval of the material accessed.

h. Access at the next higher level shall not be authorized for **COMSEC**, **SCI**, **NATO**, or foreign government information.

i. The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved

(1) The name, and SSN of the employee afforded higher level access.

(2) The level of access authorized.

(3) Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be **furthered**.

(4) An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded

(5) A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

(6) The approving authority's signature **certifying** (1) through (5), above.

(7) Copies of any pertinent **briefings/debriefings** administered to the employee.

3-407 Access by Retired Flag and/or General Officers

a. Upon determination by an active duty flag/general officer that there are compelling reasons, **in** furtherance of the Department of Defense mission, to grant a retired flag/general officer access to classified information in connection with a specific DoD program or mission, for a period not greater than 90 days, the investigative requirements of this **Regulation** may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement - not including access to SCI.

b. The flag/general officer approving issuance of the clearance **shall**, provide the appropriate DoD Component central clearance **facility** a written record to be incorporated into the **DCII** detailing

(1) Full **identifying data pertaining** to the cleared **subject**;

(2) The classification of the information to which access was authorized.

c. Such access maybe granted only after the compelling reason and the specific aspect of the DoD mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a government **installation** or other area approved for storage of **DoD** classified information.

Section 5

SPECIAL ACCESS PROGRAMS

3-500 General

It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, **national** regulations, or international agreement or Executive Order 12968 or its successor. In this connection, there are certain special access programs (SAPS) originating at the national or international level that require personnel security investigations and procedures of a special nature. Those programs and the special investigative requirements imposed by them are described in this section. A SAP is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to E. O. 12958 (reference **(j)**) and prior Executive orders. DoD Directive 0-5205.7 (reference **(qq)**) prescribes policy and procedures for establishment administration and reporting of Departmental SAPS.

3-501 Sensitive Compartmented Information (SCI)

a. The investigative requirements for access to **SCI** is an SBI (See paragraph 4, Appendix B) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate **family** (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the Personnel Security standards of **DCID** 1/14 (reference (1)) are met.

b. A previous investigation conducted within the past five years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individual's military service, DoD civilian **employment**, or access to classified information under the Industrial Security Program greater than 24 months. The individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI and/or SSBI and **certify** any substantive changes that may have occurred.

c. In accordance with DCID 1/14 (reference (l)), a TOP SECRET security clearance shall not be a prerequisite for access to **SCI**. Determination of eligibility for access to SCI under reference (1) shall include eligibility for access to TOP SECRET and below.

3-502 Single Integrated Operational Plan-Extreme ly Sensitive Information (SIOP-ESI)

The investigative requirement for access to **SIOP-ESI** is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are United States citizens other than by birth or who are resident aliens.

3-503 Presidential Support Activities

a. DoD Directive 5210.55 (reference (r)) prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DoD military and civilian personnel and contractor employees assigned to or utilized in Presidential Support activities. The type of investigation of individuals assigned to Presidential Support activities varies according to whether the person investigated qualifies for **Category One** or **Category Two** as indicated below:

(1) Category One

(a) Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office **staff of** the Director, **White** House Military Office, and all individuals under his control):

- 1 Presidential air crew and associated maintenance and security personnel.
- 2 Personnel assigned to the White House communications activities and the Presidential retreat.
- 3 White House transportation personnel.
- 4 Presidential mess attendants and medical personnel.
- 5 Other individuals filling administrative positions at the White House.

(b) Personnel assigned on a temporary or part-time basis to duties supporting the President

- 1 Military Social Aides.
- 2 Selected security, transportation, flight-line safety, and baggage personnel.
- 3 Others with similar duties.

(c) Personnel assigned to the Office of the Military Aide to the Vice President.

(2) Category Two

(a) Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential **functions** and facilities.

(b) Employees of contractors who provide services or contractors employees who require unescorted access to Presidential Support areas, activities, or equipment-including maintenance of the Presidential **retreat**, communications, and aircraft.

(c) Individuals in designated units requiring a lesser degree of access to the President or Presidential Support activities.

b. Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the spouse and all members of the individual's immediate **family** of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential Support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

c. Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and **all** members of the individual's immediate **family** of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The **BI** must have been completed within the 12 months preceding selection for Presidential Support duties. It should be noted that duties (separate and distinct **from** their Presidential Support responsibilities) of some Category Two personnel **may** make it necessary for them to have special access clearances which require an **SBI**.

d. The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation.

e. A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as "**Category A**." These personnel shall be investigated under special scoping in accordance with the requirements of reference (jj).

3-504 Nuclear **Weapon** Personnel Reliability Program (PRP)

a. DoD Directive 5210.42 (reference (s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

(1) Critical Position: **BI**. In the event that it becomes necessary to consider an individual for a critical position and the required **BI** has not been **completed**, interim certification maybe made under carefully controlled conditions as set forth below.

(a) The individual has had a favorable **DNACI**, NAC (or **ENTNAC**) within the past 5 years without a break in service or employment in excess of I year.

(b) The **BI** has been requested.

(c) All other requirements of the PRP screening process have been **fulfilled**.

(d) The individual is identified to supervisory personnel as being certified on an interim basis.

(e) The individual is not used in a two-man team with another such individual.

(f) Justification of the need for interim certification is documented by the certifying official.

(g) Should the BI not be completed within 150 days **from** the date of the **request**, the **certifying** official shall query the Component clearance authority, who shall ascertain **from** DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

(2) Controlled Position **DNACI/NACI**

(a) An **ENTNAC** completed for the purpose of first term enlistment or induction into the Armed Forces does not satisfy this requirement.

(b) Interim certification is authorized for an individual who has not had a **DNACI/NACI** completed within the past 5 **years**, subject to the following conditions:

1 The individual has had a favorable **ENTNAC/NAC**, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

2 A **DNACI/NACI** **has** been requested at the time of interim certification.

3 All other requirements of the PRP screening process have been **fulfilled**.

4 Should the **DNACI/NACI** not be completed within 90 days from the date of the **request**, the procedures set forth in a(l)(g), above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

(3) Additional requirements apply.

(a) The investigation upon which certification is based must have been completed within the last 5 years from the date of initial assignment to a PRP position and there must not have been a break in service or employment in excess of 1 year between completion of the investigation and initial assignment.

(b) In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of 1 year subsequent to completion of the investigation, a reinvestigation is required.

(c) Subsequent to initial assignment to the PRP, reinvestigation is not required so long as the individual remains in the PRP

(d) A medical evaluation of the individual as set forth in DoD Directive 5210.42 (reference (s)).

(e) Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

(f) A personal interview with the individual for the purpose of informing him of the significance of the **assignment**, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the **PRP**.

(g) Service **in the Army**, Navy and Air Force Reserve does not constitute active service for PRP purposes.

3-505 Access to North Atlantic **Treaty Organization (NATO)** Classified Information

a. Personnel assigned to a NATO staff Position requiring access to NATO COSMIC (TOPSECRET)s SECRET or **CONFIDENTIAL** information shall have been the: subject of a favorably adjudicated BI (1 O year

scope), **DNACI/NACI** or **NACI ENTNAC**, current within five years prior to the assignment, in accordance with USSAN Instruction 1-69 (reference **(kk)**) and paragraph 3-705, below.

b. **Personnel** not assigned to a NATO staff position, but requiring access to NATO COSMIC, SECRET or CONFIDENTIAL information in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate personnel security investigation (Appendix B) required by paragraph 3-401 and 3-709 of this Regulation.

3-506 Other Special Access Programs (SAPS)

Special investigative requirements for **SAPs** not provided for in this paragraph may be established only as part of the written program approval of the Deputy Secretary of Defense in accordance with the SAP approval process prescribed for in DoD Directive 0-5205.7 (reference **(qq)**).

Section 6

CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION

3-600 General

DoD Directive 5200.8 (reference (t)) outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of properly or places under their command. Essential to carrying out this responsibility is a commander's need to protect the **command** against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this Regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if **performed** by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

3-601 Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information

a. Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be **limited** to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or **ENTNAC**) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate component agency or activity prior to permitting such access. DoD Components shall not **request**, and shall not direct or permit their contractors to **request**, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In **determining** trustworthiness under this paragraph, the provisions of paragraph 2-200 and **Appendix I** will be utilized.

b. In meeting the requirements of this paragraph, approval shall be obtained **from** one of the authorities designated in paragraph A, Appendix F of this Regulation, for authority to request NACS on DoD military, civilian or contractor employees. A justification shall accompany each request which shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

c. NAC requests shall (1) be forwarded to DIS in accordance with the provisions of paragraph B, Appendix C, (2) contain a reference to this paragraph on the DD Form 398-2, and (3) list the authority in Appendix F who approved the request.

d. Determinations to deny access under the provisions of this paragraph must not be exercised in an **arbitrary**, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DoD Directive 5200.8 (reference (t)).

3-602 Nonappropriated Fund Employees

Each **Nonappropriated** Fund employee who is employed in a position of trust as designated by an official authorized in paragraph H, Appendix F, shall have been the subject of a NAC completed no longer than 12 months prior to **employment** or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DoD Manual 1401.1-- (reference (u)). An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. **Issuance** of a CONFIDENTIAL or SECRET clearance will be based on a **DNACI** or NACI in accordance with paragraph 3-401.

3-603 Customs Inspectors

DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49-R (reference (v)), shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DoD employment greater than 1 year in which case a current NAC is required.

3-604 Red Cross/United Service Organizations Personnel

A **favorably** adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as prerequisite for assignment with the Armed Forces overseas (DoD Directive 5210.25 (reference (w))).

3-605 Officials Authorized to Issue Security Clearances

Any person authorized to adjudicate **personnel** security clearances shall have been the subject of a favorably adjudicated BI.

3-606 Personnel Security Clearance adjudication Officials

Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated **BI**.

3-607 Persons Requiring DoD Building Passes

Pursuant to DoD Directive 5210.46 (reference (z)), each person determined by the designated authorities of the Components concerned as having an official need for access to DoD buildings in the National Capital Region shall be the subject of a favorably, adjudicated NAC prior to issuance of a DoD building pass. Conduct of a **BI** for this purpose is prohibited unless approved in advance by **ODUSD(P)**.

3-608 Foreign National Employees Overseas Not Requiring Access to Classified Information

Foreign nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate military department investigative organization consistent with paragraph 2-404, prior to employment

a. Host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and

b. DCII

c. **FBI-HQ/ID** (Where information exists regarding residence by the foreign national in the United States for one year or more since age 18)

3-609 **Special Agents and Investigative Support Personnel**

Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

3-610 **Persons Requiring Access to Chemical Agents**

Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DoD Directive 5210.65 (reference (y)).

3-611 **Education and Orientation Personnel**

Persons selected for duties in connection with programs involving the education and orientation of **military** personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include **teachers/administrators** associated with **university** extension courses conducted on military installations in the United States. Non-US citizens **from** a country listed in Appendix H **shall** be required to undergo a **BI** if they are employed in a position covered by this paragraph.

3-612 **Contract Guards**

Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC prior to such assignment.

3-613 **Transportation of Arms, Ammunition and Explosives (AA&E)**

Any DoD military, civilian or contract employee (including commercial **carrier**) operating a vehicle or providing security to a vehicle transporting Category I, II or CONFIDENTIAL AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC.

3-614 **Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II & ADP-III**

DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix K) and investigated as follows:

ADP-I:	BI
ADP-II:	DNACI/NACI
ADP-III:	NAC/ENTNAC

Those personnel falling in the above categories who require access to classified information will, of course, be subject to the appropriate investigative scope contained in paragraph 3-401, above.

3-615 Others

Requests for approval to conduct an investigation on other personnel, not provided for in paragraphs 3-601 through 3-614, above, considered to fall within the general provisions of paragraph 3-600 above, shall be submitted, detailing the justification **therefor**, for approval to **the** Deputy Under Secretary of Defense for Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

Section 7

REINVESTIGATION

3-700 General

DoD policy prohibits unauthorized and unnecessary investigations. **There** are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under **the** provisions of this Regulation. It is the policy to limit reinvestigation of individuals to the scope contained in **paragraph 5, Appendix B to meet** overall security requirements. Reinvestigation generally, is authorized only as follows:

- a. To prove or disprove an allegation relating to the criteria set forth in paragraph 2-200 of this Regulation with respect to an individual holding a security clearance or assigned to a position that requires a trustworthiness determination;
- b. To meet the periodic reinvestigation requirements of this regulation with respect to those security programs enumerated below; and
- c. Upon individual **request**, to assess the current eligibility of individuals who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

3-701 Allegations Related to Disqualification

Whenever questionable behavior patterns develop, derogatory information is **discovered**, or inconsistencies arise related to the disqualification criteria outlined in paragraph 2-200 that could have an adverse impact on an individual's security status, a Special Investigative Inquiry (**SII**), psychiatric, drug or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative **subject**, and the subject fails to **furnish** the required **data**, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph 8-201 of this Regulation.

3-702 Access to Sensitive Compartmented Information(SCI)

Each individual having current access to **SCI** shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-703 Critical-sensitive Positions

Each DoD civilian employee occupying a critical sensitive position shall be the subject of a PR conducted **an** a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-704 Presidential Support Duties

Each individual assigned Presidential Support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-705 NATO Staff

Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

3-706 Extraordinarily Sensitive Duties

In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special compartmentation and other special security measures. In such instances, a Component SOIC may, with the approval of the **Deputy** Under Secretary of Defense for Policy, request **PR's** at intervals of less than 5 years as **outlined in** paragraph 5, Appendix B. Such requests shall include full justification and a recommendation as to the desired **frequency**. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

- a. The potential damage that might result from the individual's defection or abduction.
- b. The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the **individual's** suitability for continued **SCI** access.

3-707 Foreign Nationals Employed by DoD Organizations Overseas

Foreign nationals employed by DoD organizations overseas who have been granted a "Limited Access Authorization" pursuant to paragraph 3-402 shall be the subject of a **PR**, as set forth in paragraph 5, Appendix B, conducted under the auspices of DIS by the appropriate military department or other U.S. Government investigative agency consistent with paragraph 2-404 and Appendix J of this Regulation.

3-708 Persons Accessing Very Sensitive Information Classified Secret

a.. Heads of **DoD** Components shall submit a request to the Deputy Under Secretary of Defense for Policy for approval to conduct periodic reinvestigations on persons holding Secret clearances who are exposed to very sensitive Secret information.

b. Generally, the **Deputy** Under Secretary of Defense for Policy will only approve periodic reinvestigations of persons having access to Secret information if the unauthorized disclosure of the information in question could reasonably be expected to:

- (1) Jeopardize human life or safety.
 - (2) Result in the loss of unique or uniquely productive intelligence sources or methods vital to U.S. security.
 - (3) Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.
- c. Each individual accessing very sensitive Secret information who has been designated by a **authority** listed in paragraph A, **Appendix F** as requiring periodic reinvestigation, **shall** be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph 5, Appendix B.

3-709 Access to **Top Secret Information**

Each individual having current access to Top Secret information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph 5, Appendix B.

3-710 Personnel **Occupying Computer Positions Designated ADP-1**

All DoD military, civilians, consultants, and contractor personnel occupying computer positions designated **ADP-I**, shall be ~~the~~ subject of a PR conducted on a 5-year recurring basis as set forth in paragraph 5, Appendix B.

Section 8

AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS

3-800 Authorized **Officials**

Only an official designated in paragraph G, Appendix F, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this chapter. Such waiver **shall** be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DoD mission. A minor investigative element that has not been met should not preclude favorable adjudication--nor should this require a waiver when **all** other **information** developed on an individual during the course of a prescribed investigation is favorable.

CHAPTER IV

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

4-100 General

Investigations conducted by DoD organizations or another Agency of the Federal Government shall not be duplicated when those investigations meet the scope and standards for the level of the clearance or access required. The DoD Components that grant access (SCI or SAP) or issue security clearances (TOP SECRET, SECRET, and **CONFIDENTIAL**) to civilian **and/or** military or contractor employees are responsible for determining whether such individuals have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance or access, which is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance or access **required**, shall provide the basis for issuance of a new clearance and/or access without further investigation or adjudication. Previously conducted investigations and previously rendered personnel security determinations shall be accepted within the Department of Defense, in accordance with the policy in sections 4-101 through 4-103 below.

4-101 Prior Personnel Security Investigations

As long as there is no break in Military Service and/or Federal employment greater than 24 months, any previous personnel security investigation that essentially is equivalent in scope to an investigation required by this Regulation will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of paragraphs 2-307 and 4- 102.b. of this Regulation.

4-102 Prior Personnel Security Determinations Made by DoD Authorities

a. Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to **SCI**) made by designated DoD authorities will be mutually and reciprocally accepted by all DoD Components without requiring additional investigation, unless there has been a break in the individual's Military Service and/or Federal employment of greater than 24 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the **DCII** or other appropriate databases should be conducted to accomplish this task.

b. Whenever a valid DoD security clearance or access eligibility is on record, Components shall not request DIS or other DoD investigative organizations to forward prior investigative files for review unless:

(1) Significant derogatory information or investigation completed subsequent to the date of last clearance and/or an access authorization, is known to the **requester**; or

(2) The individual concerned is being considered for a higher level clearance (e.g., Secretor Top Secret) or the individual does not have **an** access authorization **and** is being considered for one; or

(3) The most recent clearance or access authorization of the individual concerned was conditional or based on a waiver.

c. Requests for prior investigative files authorized by this Regulation shall be made in writing, shall cite the specific justification for the request (i.e., upgrade of clearance, issue Special Access authorization, etc.), and shall include the date, level, and issuing organization of the individual's current or most recent security clearance or Special Access authorization.

d. All requests for **non-DoD** investigative files, authorized under the criteria prescribed by paragraphs a, b(1), (2), (3), and (4) and c, above, shall be:

(1) Submitted **on** DD Form 398-2 to DIS;

(2) Annotated as a "Single Agency Check" of whichever agency developed the investigative file or to obtain the check of a single national agency.

e. When further investigation is desired, in addition to an existing **non-DoD** investigative file, a DD Form 1879 **will** be submitted to DIS with the appropriate security forms attached. The submission of a Single Agency Check via DD Form 398-2 will be used to obtain an existing investigative file or check a single national agency.

f. Whenever a civilian or military member transfers from one DoD activity to another, the losing organization's security **office** is responsible for advising **the** gaining organization of any pending action to suspend, deny or revoke the individual's security clearance as well as any adverse information that may exist in security, personnel or other files. In such instances the clearance shall not be reissued until the questionable information has been adjudicated.

4-103 Investigations Conducted and Clearances Granted by Other Agencies of the Federal Government

a. Whenever a prior investigation or **personnel** security determination (including clearance for access to information classified under Executive Order 12356 (reference (j))) of another agency of the Federal Government meets **the** investigative **scope** and standards of this Regulation, such investigation or clearance may be accepted for the investigative or clearance purposes of this Regulation, provided that the employment with the Federal agency concerned has been continuous and there has been no break longer than 24 months since completion of the prior investigation, and further provided that inquiry with the agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation **shall** be requested.

b. A **NACI** conducted by OPM shall be accepted and considered equivalent to a **DNACI** for the purposes of this Regulation.

c. Department of Defense policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set forth in DoD Directive 5210.2 (reference (z)).

CHAPTER VII

ISSUING CLEARANCE AND GRANTING ACCESS

7-100 General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual **is** eligible for access to Special Access program **information**, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a **function** distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified **information** in order to **perform** official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8-102.

b. Only the authorities designated in Paragraph A, Appendix F are authorized to **grant**, deny or revoke personnel security clearances or Special Access authorizations (other than **SCI**). Any commander or head of **an** organization may suspend access for cause when there exists **information** raising a serious question as to the individual's ability or intent to protect classified **information**, provided that the procedures set forth in paragraph 8-102 of this Regulation are complied with.

c. All commanders and heads of DoD organizations have the responsibility for determining those position **functions** in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Regulation.

7-101 Issuing Clearance

a. Authorities designated in Paragraph A, Appendix F shall record the issuance, denial, or revocation of a personnel security clearance in the **DCII** (see paragraph 6-103, above). A record of the clearance issued shall also be recorded in an individual's **personnel/security** file or official personnel folder, as appropriate.

b. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated **from** DoD civilian employment, (3) has no **further** official relationship with DoD, (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with DoD exists greater than 24 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance

shall be reissued without **further** investigation or adjudication provided there has been no additional investigation or development of derogatory information.

c. Personnel security clearances of DoD military personnel shall be granted, denied, or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on **Army**, Navy, and Air Force personnel by DIS will be returned only to the parent service of the subject for adjudication regardless of the source of the original request. The adjudicative authority **will** be responsible for expeditiously transmitting the results of the clearance **determination**. As an **exception**, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility **determination** by the individual's parent Component. Whenever an employing DoD Component issues an interim clearance to an individual from another **Component**, written notice of the action shall be provided to the parent Component.

d. When an SSBI (or PR) for access to SCI is initiated on a military member, who is assigned to a Defense agency (except **DIA**), **OSD staff**, or the Joint Staff, DIS will return the completed investigation to the appropriate Military Department CAF, in accordance with subsection 7-101 .c., above, for issuance (or **reissuance**) of the SCI eligibility. The CAF shall be responsible for expeditiously transmitting the results of the SCI eligibility determination to the requesting Defense agency. For military personnel assigned to the DIA, the completed investigation will be forwarded to the DIA for the **SCI** eligibility determination. The DIA will expeditiously transmit the results of the **SCI** eligibility determination to the appropriate Military Department CAF.

e. When the Defense Industrial Security Clearance Office (DISCO) initiates an SSBI (or PR) for access to SCI on a contractor employee, DIS will return the completed investigation to the appropriate CAP with **SCI** cognizance. Following a favorable **SCI** eligibility determination, the CAP will **notify** DISCO of the outcome. If the SCI eligibility is denied or revoked, the CAF will complete all appropriate due process and appeal procedures before forwarding the case and all relevant additional documentation to DISCO for appropriate action, to include referral to the Defense Office of Hearings and Appeals (DOHA) for possible action under DoD Directive 5220.6 (reference (c)).

f. The interim clearance shall be recorded in the **DCII** (paragraph 6-103, above) by the parent DoD Component in the same manner as a final clearance.

7-102 Granting Access

a. Access to classified **information** shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative **function** relating

to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance **determination**, issued by any DoD authority authorized by this Regulation to issue personnel security clearance, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

c. The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (**DCII**), along with clearance eligibility. However, completion of the **DCII** Access field is required effective 10 October 1993 in all instances where the adjudicator is reasonably aware of the level of classified access associated with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible.

CHAPTER VIII

UNFAVORABLE ADMINISTRATIVE ACTIONS

Section I

REQUIREMENTS

8-100 General.

For purposes of this Regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph 1-301, and any unfavorable personnel security determination, as defined at paragraph 1-329. This chapter is intended only to provide guidance for the internal operation of the Department of **Defense** and is not intended to, does **not**, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

8-101 Referral for Action

a. Whenever derogatory information related to the criteria and policy set forth in paragraph 2-200 and Appendix I of this Regulation is developed or otherwise becomes available to any DoD **element**, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If **further** information is needed to **confirm** or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall **insure that the** appropriate Central Adjudicative Facility (**CAF**) of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or **security officer** shall in no way affect or limit the responsibility of the **CAF** to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph 8-201, below, if such action is warranted and supportable by the criteria and policy contained in paragraph 2-200 and Appendix I. No unfavorable administrative action as defined in paragraph 1-328 and 329 may be taken by the organization to which the individual is assigned for duty without affording the person the **full** range of protections contained in paragraph 8-201, below, or, in the case of SCI, Annex B, **DCID** 1/14 (reference (1)).

b. The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by **DIS**. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

8-102 Suspension

a. The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), **if** information exists which raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) **until** a final determination is made by the appropriate authority designated in Appendix F.

b. Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), **the** individual concerned must be notified of the determination in writing by the commander, or component CAP, to include a brief statement of the reason(s) for the suspension action consistent with **the** interests of **national** security.

c. Component field elements must promptly report all suspension actions to the appropriate CAF, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the **DCII** Eligibility and Access fields to alert all users to the individual's changed status.

d. Every effort shall be made to resolve suspension cases as expeditiously as circumstances permit. Suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD (**I&S**) for review and appropriate action.

e. A **final** security clearance eligibility determination shall be made for all suspension actions and the determination entered in the **DCII**. **If**, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code (adjudication action incomplete due to loss of jurisdiction) in the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code **Y**) remain as a permanent record in the **DCII**.

f. A clearance or access entry in the **DCII** shall not be suspended or downgraded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5-year time period for TOP **SECRET/SCI** or within the period prevailing for **SECRET** clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed **timeframe**, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

8-103 Final Unfavorable Administrative Actions

The authority to make **personnel** security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix F, except that the authority to terminate the employment of a civilian employee of a military department or Defense agency is vested solely in the head of the DoD component concerned and in such other statutory official as maybe designated. Action to terminate civilian employees of the **Office** of the Secretary of Defense and DoD **Components**, on the basis of criteria listed in paragraph 2-200, a through f, shall be coordinated with the **Chief** of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence

OASD (C3I) prior to final action by the head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (**nonsecurity**) regulations of the military departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the **CAF** to continue to process the individual for denial or revocation of a security clearance, access to classified **information**, or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this Regulation.

Section 2

PROCEDURES

8-200 General

- I No final unfavorable personnel security clearance or access determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person **affiliated** with the Department of Defense without granting the individual concerned the procedural benefits set forth in 8-201 below, when such determination results in an unfavorable administrative action (see paragraph 8-100). As an exception, DoD contractor personnel shall be afforded the procedures contained in DoD Directive 5220.6 (reference (c)) and Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DoD Directive 5210.25 (reference (w)). Procedures for unfavorable decisions regarding access to SAPS may differ from the procedures in this Regulation as authorized in **E.O. 12968** and as approved by the Secretary of Defense or Deputy Secretary of Defense.

8-201 Unfavorable Administrative Action Procedures

Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the individual concerned has been:

- a. Provided a written statement of the reasons (**SOR**) as to why the unfavorable administrative action is being taken in accordance with the example at Appendix L, which includes sample letters and enclosures. The SOR shall be as comprehensive and detailed as the protection of sources afforded **confidentiality** under provisions of the Privacy Act of 1974 (reference (m)) and national security permit. The statement will **contain**, 1) a summary of the security concerns and supporting adverse information, 2) instructions for responding to the SOR and 3) copies of the relevant security guidelines from Appendix I. In addition, the CAF will provide within 30 calendar days, upon request of the individual, copies of releasable records of the personnel security investigation (the CAF must retain copies of the file for at least 90 days to ensure the ready availability of the material for the subject). If the CAF is unable to provide requested documents for reasons beyond their control, then the name and address of the agency (agencies) to which the individual may write to obtain a copy of the records will be provided.

- (1) The head of the local organization of the individual receiving an SOR shall designate a point of contact (**POC**) to serve as a liaison between the CAF and the individual. The duties of the POC will include, but not necessarily be limited to, delivering the SOR, having the individual acknowledge receipt of the SOR, determining whether the individual intends to respond within the time specified; ensuring that the individual understands the consequences of the proposed action as well as the consequences for failing to respond in a timely fashion; explaining how to obtain time extensions, procure copies of investigative records, and the procedures for responding to the SOR; and ensuring that

the individual understands that he or she can obtain legal counselor other assistance at his or her own expense.

b. Afforded an opportunity to reply in writing to the CAF within 30 calendar days from the date of receipt of the SOR. Failure to submit a timely response will result in forfeiture of all future appeal rights with regard to the unfavorable administrative action. Exceptions to this policy may only be granted by the CAP in extraordinary circumstances where the individual's failure to respond to the SOR was due to factors beyond his or her **control**. The CAP must be notified of the individual's intent to respond, via the POC, within 10 calendar **days** of receipt of the SOR. An extension of up to 30 calendar days may be granted by the employing organization following submission of a written request from the individual. Additional extensions may only be granted by the CAP. Responses to the CAP must be forwarded through the head of the employing organization.

c. Provided a written response by the CAP to any submission under subparagraph b. stating the final reason(s) for the unfavorable administrative action, which shall be as specific as privacy and national security considerations permit and in accordance with the example of a letter of **denial (LOD)** and its enclosures at Appendix L. Such response shall be as prompt as individual circumstances **permit**, not to exceed 60 calendar days from the date of receipt of the response submitted under subparagraph b., above, provided no additional investigative action is necessary. If a final response cannot be completed within the time **frame allowed**, the individual must be notified in writing of this **fact**, the reasons therefor, and the date a final response is **expected**, which shall not normally exceed a total of 90 days from the date of receipt of **the** response under subparagraph b.

d. Afforded an opportunity to appeal an LOD, issued pursuant to paragraph c. above, to the component Personnel Security Appeals Board (**PSAB**). The PSAB shall consist of a minimum of three members and **function** in accordance with Appendix M. If a decision is made to appeal the LOD, the individual may do so by one of the following methods:

(1) **Appeal Without a Personal Appearance:** Advise the PSAB within 10 calendar days of receipt of the LOD, of the intent to appeal. Within 40 calendar days of receipt of the LOD, write to the appropriate PSAB stating reasons why the LOD should be overturned and providing any additional, relevant **information** that may have a bearing on the final decision by the PSAB;

(2) **Appeal With a Personal Appearance:** Advise the Defense Office of Hearings and Appeals (DOHA) within 10 calendar days of receipt of the LOD that a personal appearance before a DOHA Administrative Judge (**AJ**) is desired in order to provide additional, relevant information which may have a bearing on the final decision by the PSAB. DOHA will promptly schedule a personal appearance and will provide a recommendation to the PSAB generally within 60 days of receipt of the notice requesting the personal appearance. Procedures governing the conduct of the personal appearance before a DOHA AJ are contained at Appendix N.

e. Provided a final written decision by the PSAB, including a rationale, to any submission under subparagraph d., above, stating the final disposition of the appeal. This will normally be accomplished within 60 calendar days of receipt of the written appeal from the individual if no personal appearance was requested, or within 30 calendar days from receipt of the AJ's recommendation if a personal appearance was requested.

8-202 Due Process Review

The due process and appeal procedures will be reviewed one year after implementation. The above procedures will become effective no later than 120 days after the date of this change.

8-203 Exceptions to Policy

Notwithstanding paragraph 8-201 above or any other provision of this **Regulation**, nothing in this Regulation shall be deemed to limit or **affect** the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national **security** so requires, pursuant to Section 7532, Title 5, United States Code (reference **(pp)**). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph 8-201 above are not appropriate. Such determination shall be conclusive.

Section 3

REINSTATEMENT OF CIVILIAN EMPLOYEES

8-300 General

Any person whose civilian employment in the Department of Defense is terminated under the provisions of this Regulation **shall** not be reinstated or restored to duty or reemployed in the Department of Defense unless the Secretary of Defense, or the head of a DoD **Component**, finds that such reinstatement restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

8-301 Reinstatement Benefits

A DoD civilian employee whose employment has been suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Section 3571 of Title 5, U.S. Code (reference (old)) is entitled to benefits as provided for by Section 3 of Public Law 89-380 (reference **(ee)**).

CHAPTER XII

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX

12-100 General

a. The Defense Clearance and Investigations Index (**DCII**) is the single, automated central repository that identifies investigations conducted by DoD investigative Agencies, and personnel security determinations made by DoD adjudicative authorities.

b. The **DCII** data base consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by **subject**, in the **DCII**.

c. **DoD** investigative and adjudicative authorities report information which is used for investigative, adjudicative, statistical, research and other purposes as authorized by **OASD(C3I)** approval.

12-101 Access

The **DCII** is operated and maintained by the Defense Investigative Service (**DIS**). Access is normally limited to the Department of Defense and other Federal Agencies with adjudicative, investigative and/or counterintelligence (**CI**) missions. Agencies wishing to gain access to the **DCII** must submit a written request outlining specific requirements with corresponding justification, as stated in paragraph 12-101.a. through 12-101 .d. below. On approval, a Memorandum of Understanding (**MOU**) addressing **equipment**, maintenance, security, privacy, and other agency responsibilities shall be forwarded to the requester by DIS for signature.

a. Military Departments. Requests **from** military departments or organizations must be submitted for approval and endorsement through the following **offices** to DIS, Director, National Computer Center, **P.O.** Box 1211, Baltimore, MD 21203-1211.

(1) Air Force. Administrative Assistant to the Secretary of the Air Force, Pentagon, Room 4D881, Washington, DC 20330-4000.

(2) Army. Director, Counterintelligence and Security Countermeasures, Office of the Deputy Chief of Staff for Intelligence, Department of the Army, Pentagon, Room **2D48I**, Washington, DC 20301-1050.

(3) Navy and Marine Corps. Director, Information and Personnel Security Policy Directorate, Naval Criminal Investigative Service, Chief of Naval Operations (**OP-09N**), Washington, DC 20350-2000.

b. Unified Combatant Commands. Requests from Unified Combatant Commands must be submitted for approval to DIS, Director, National Computer Center through the Joint Chiefs of Staff,

Chief, Security Division, Directorate for Information and Resource **Management**, The Joint Staff, Room 1B738, The Pentagon, Washington DC 20318-9300.

c. Defense Agencies. Requests from DoD Agencies must be submitted through, and with the approval **of**, the agency's Security Headquarters Office to DIS, Director, National Computer Center, PO Box 1211, Baltimore, MD 21203-1211.

d. **Non-DoD** Agencies. Requests from **Non-DoD** agencies must be submitted to the Deputy Assistant Secretary of Defense (Intelligence and Security), Attn: Counterintelligence and Security Programs, Room **3C281**, 6000 Defense **Pentagon**, Washington, DC 20301-6000. On approval, those requests shall be forwarded to the DIS for action.

12-102 Investigative Data

Contributors to the DCII shall ensure that all investigative data on an individual is entered into the **DCII**.

a. An entry shall be made to indicate a pending investigation when an investigation is opened.

b. When an investigation has been **completed**, the contributor shall change the **DCII** status to reflect a completed investigation, including the date (year) of the investigation.

c. Changes or additions to existing files **must**, whenever appropriate, all be reflected in the **DCII**.

d. Investigative file tracings maybe deleted **from** the **DCII** when the retention period is over and the record file has been destroyed.

12-103 Adjudicative Data

All adjudicative determinations on personnel with access to classified information or performing sensitive duties shall be indexed in the **DCII**.

a. Specifically, a **DCII** clearance entry shall be created or updated as follows:

(1) Immediately upon suspension of access.

(2) When interim access has been authorized by the CAF or employing activity.

(3) Immediately following the granting, denial, or revocation of a clearance or access.

(4) Following the **receipt**, review, and adjudication of information received subsequent to the prior clearance or access determination.

b. **DCII** entries shall inform the DoD Components of the clearance eligibility and/or access status of an individual or the presence of an adjudicative file.

c. An adjudicative determination shall remain in the **DCII** as long as the subject is **affiliated** with the Department of Defense. **The** determination may be deleted 2 years after the employment and/or

clearance eligibility ends. The deleted DCII data shall be retained by the DIS in a historical file for a minimum of 5 years after deletion by the contributor.

d. The date of the **DCII** clearance and/or access entry shall always be the same as or subsequent to the date of the most recent investigation.

e. DoD Components will **notify** the **CAF** of applicable personnel changes to ensure the accuracy of the DCII data base.

12-104 Notification to Other Contributors

Whenever a DoD contributor to the **DCII** becomes aware of significant unfavorable information about an individual with a clearance and/or access entry **from** another DoD contributor, immediate notification must be made to the latter along with copies of all relevant information.

12-105 Security Requirements for the DCII

a. **The DCII** is an unclassified system that meets the C-2 level of protection under the Computer Security Act of 1987. Contributors may enter only unclassified **information**.

b. Information contained in the **DCII** receives the protection required by the Privacy Act of 1974. (reference m)

(1) Due to the sensitive nature of the information, positions having direct (password) access to a **DCII** terminal are considered to be **ADP-I** Critical Sensitive Positions.

(2) Individuals authorized access to the **DCII** must have a favorably completed **SSBI** (or **BI** and/or **SBI**).

(3) DoD activities and other Federal Agencies that have been authorized "Read Only" access to the **DCII** must also comply with those investigative requirements.

c. Each authorized contributor is responsible for the accuracy of the data it enters. Contributors may enter, **modify** or delete only data originated by them. The **DCII** shall not allow one contributor to alter or delete another contributor's information.

d. To prevent unauthorized access or tampering during nonworking hours, **DCII** terminals must be located in an area that is secured by guard personnel, an alarm system, or appropriate locking device.

e. When the **DCII** terminal is operational, access to **DCII** information shall be controlled and limited to those persons authorized access to that information.

12-106 Disclosure of Information

The Privacy Act of 1974 requires an accounting of the disclosure of personal information when it is provided to another Agency. For accessing the **DCII**, the Department of Defense is considered a single Agency. Disclosure of personal information in the Department of Defense does not require specific accounting for each disclosure. All releases of information obtained from the **DCII** to any non-DoD source must be recorded in the DCII Disclosure Accounting System (**DDAS**) by the Agency that

releases the information. A contributor may disclose only the DCII data originated by that contributor to the subject of the data. Requests for release of investigative reports or adjudicative files are handled as Privacy Act requests by contributors.

APPENDIX A

REFERENCES, continued

- (e) Public Law 88-290, 'National Security Agency - Personnel Security Procedures,' March 26,1964 (78 STAT. 168)
- (f) Public Law 86-36, "National Security **Agency-Officers and Employees,**" May 29,1959 (73 Stat. 63)
- (g) Executive Order 10450, "**Security** Requirements for Government Employment" April 27,1953
- (h) Executive Order 12333, "United States Intelligence Activities; December 4,1981
- (i) DoD Directive 5210.45, "Personnel Security in the National Security **Agency,**" May 9, 1964
- (j) Executive Order 12958, "Classified National Security Information," April 17, 1995
- (k) Executive Order 11935, "Citizenship Requirements for Federal **Employment,**" September 2, 1976
- (l) Director of Central Intelligence Directive (**DCID**) No. 1/14, "Personnel **Security** Standards and Procedures Governing Eligibility for Access to Sensitive **Compartmented** Information (**SCI**)," January 22, 1992
- (m) Section 552a of title 5, United States Code
- (n) DoD Directive 5100.23, "Administrative Arrangements for the National Security **Agency,**" May 17, 1967
- (o) Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation April 5, 1979
- (p) DoD Directive 5210.48, "DoD Polygraph **Program,**" December 24, 1984
- (q) DoD **5200.1-R,** "Information Security Program **Regulation,**" June 1986, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
- (r) DoD Directive 5210.55, "Selection of **DoD** Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support **Activities,**" July 6, 1977
- (s) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability **Program,**" May 25,1993
- (t) DoD Directive 5200.8, "Security of Military Installations and **Resources,**" April 25,1991
- (u) DoD 1401. 1-M, "**Personnel** Policy Manual for Nonappropriated Fund **Instrumentalities,**" January 1981, authorized by DoD Instruction 1401.1, November 15, 1985
- (v) DoD **5030.49-R,** "Customs Inspection," May 1977, authorized by DoD Directive 5030.49, January 6, 1984
- (w) DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc, Employees to Duty with the Military **Services,**" May 12, 1983
- (x) DoD Directive 5210.46, "DoD Building Security for the National Capital Region," January 28, 1982
- (y) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986
- (z) DoD Directive 5210.2, "Access to and Dissemination of Restricted **Data,**"

- January 12, 1978
- (aa) DoD Directive 5400.7, “DoD Freedom of Information Act **Program**,” May 13, 1988
 - (bb) DoD Directive 5400.11, “Department of Defense Privacy Program,” June 9, 1982
 - (cc) 5 **CFR**, Part 732, “_National Security **Positions**,” January 1, 1995
 - (old) Section 3571 of title 5, United States Code
 - (ee) Section 3 of Public Law 89-380, “Back Pay Act of **1966**,” March 30, 1966
(80 Stat. 94)
 - (ff) Executive Order 9835, “Prescribing Procedures **for the** Administration of an Employee Loyalty Program in the Executive **Branch** of the Government” issued 1947 (superseded by Executive Order 10450)
 - (gg) Public Law 83-703, “Atomic Energy Act of **1954**,” as amended, **August** 30, 1954
 - (hh) DoD Directive 5105.42, “Defense Investigative Service,” June 14, 1985
 - (ii) Defense Investigative Service 20-1-M, “Manual for Personnel Security **Investigations**,” January 1993
 - (ii) Memorandum of Understanding between the Director, White House Military **Office** and the Special Assistant to the Secretary and Deputy Secretary of Defense, “White House Clearances July 30, 1980
 - (kk) USSAN Instruction 1-69, April 21, 1982 (Enclosure 2 to DoD Directive 5100.55, “United States Security Authority for North Atlantic Treaty Organization Affairs,” April 21, 1982
 - (ll) DoD Directive 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations,” June 16, 1982
 - (mm) DoD Directive 5100.3, “Support of the Headquarters of Unified, Specified, and Subordinate Joint **Commands**,” November 1, 1988
 - (nn) Public Law 96-456, “Classified Information Procedures **Act**,” October 15, 1980 (94 Stat. 2025)
 - (oo) DoD Directive 5142.1, “Assistant Secretary of Defense (Legislative **Affairs**),” July 2, 1982
 - (pp) Section 7532 of title 5, United States Code
 - (qq) DoD Directive 0-5205.7, “Special Access Program (SAP) **Policy**,” January 4, 1989
 - (rr) National Security Directive 63, “Single Scope Background Investigations; October 21, 1991

APPENDIX B

INVESTIGATIVE SCOPE

This appendix prescribes the scope of the various types of personnel security investigations.

1. National Agency Check (NAC). The scope for NAC is five years or to age 18, whichever is the shorter period. At a minimum, the first three of the described agencies (**DCII**, **FBI/HQ**, and **FBI/ID**) below shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described agencies, if appropriate.

a. The **DCII** data base consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by subject, in the **DCII**. **DCII** records will be checked on all subjects of DoD investigations.

b. **FBI/HQ** has on file copies of investigations conducted by the FBI. The **FBI/HQ** check, included in every NAC, consists of a review of files for information of a security nature and that developed during applicant-type investigations.

c. An **FBI/ID** check, included in every NAC (but not ENTNAC), is based upon a technical fingerprint search that consists of a classification the subject's fingerprints and comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

d. **OPM**. The files of OPM contain the results of investigations conducted by OPM under E.O. 9835 and 10450 (references (ff) and (g)), those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and those requested since August 1952 to serve as a basis for "Q" clearances. OPM records are checked on **all** persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or the DOE.

e. Immigration and Naturalization Service (**I&NS**). The files of **I&NS** contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declaration of intention, visitors' visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the U.S. **I&NS** records are checked when the subject is:

(1) An alien in the U. S., or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

(4) A U.S. citizen who receives derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

f. State Department. The State Department maintains the following records:

(1) Security Division (S/D) files contain information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

(2) Passport Division (P/D) shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where he was born. Verification of this registration is verification of citizenship.

g. Central Intelligence Agency (CIA). The CIA maintains the following records:

(1) Directorate of Operations (CIA-DO/IMS) maintains the Foreign Intelligence/Counterintelligence database. This database shall be checked for all aliens residing outside the U.S. requiring access to classified information (i.e., **LAA**). If the requester provides complete personal **identifying** information (Complete Name, Date of Birth, Place of Birth, and Citizenship), all alien co-subjects (on **SSBIs**) residing outside the U.S. are also checked. In addition, this database shall be queried on the Subject any time there is a counterintelligence concern raised during the conduct of the personnel security investigation.

(2) Office of Security (CIA-SEC) maintains information on present and former employees, including members of the **Office** of Strategic Services (OSS), and applicants for employment. These files **shall** be checked if subject has been an employee of the CIA or when other sources indicate that CIA may have pertinent information.

h. Military Personnel Record Center files are maintained by separate departments of the Armed Forces, General Services Administration and the Reserve Records Centers. They consist of the Master Personnel Records of retired, separated, reserve, and active duty members of the Armed Forces. These records shall be checked when the requester provides required **identifying** data indicating service during the last 5 years.

i. Treasury Department. The files of Treasury Department agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) will be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

j. The files of other agencies such as the National Guard Bureau, the Defense Industrial Security Clearance **Office** (DISCO), etc., will be checked when pertinent to the purpose for which the investigation is being conducted.

2. **Single Scope Background Investigation (SSBI):**

The following SSBI scope reflects the requirements of National Security Directive 63 (reference (rr)).

a. **Scope:** The period of investigation for an SSBI is the last ten (10) years or to age 18, whichever is the shorter period, **provided that the investigation** covers at least the last 2 full years

of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, **employment**, and reference (including developed) contact.

b. **Expansion of Investigation.** The investigation may be expanded as necessary, to resolve issues **and/or** address employment standards unique to individual agencies.

c. **NAC.** Checks on subject and spouse/cohabitant of investigative and criminal history **files** of the Federal Bureau of Investigation, including submission of fingerprint records on the subject, and such other national agencies (**DCII**, INS, OPM, CIA, etc.). In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply.

(1) A **DCII**, FBI/ID name check only and **FBI/HQ** check shall be conducted on subject's spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's PSQ **shall** be conducted.

(2) A check of **FBI/HQ files** on members of subject's immediate family who are 18 years of age or older and who are **non-U.S.** citizens shall be conducted. As used throughout the Regulation, members of subject's immediate family include the following:

- (a) Current spouse.
- (b) Adult children, 18 years of age or older, by birth, adoption, or marriage.
- (c) Natural, adopted, foster, or stepparents.
- (d) Guardians.
- (e) Brothers and sisters either by birth, adoption, or remarriage of either parent.
- (f) Cohabitant.

(3) The files of CIA shall be reviewed on **non-U.S.** citizens of subject's immediate family who are 18 years of age or older.

(4) **I&NS files** on members of subject's immediate **family** 18 years of age or older shall be reviewed when they are:

- (a) Non-U.S. citizens, or
- (b) Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or
- (c) U.S. citizens born in a foreign country of American parent(s) or U.S. citizens who received derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

d. **Subject Interview.** Required in all cases and shall be conducted by trained security, investigative, or counterintelligence personnel to ensure **full** investigative coverage. An additional

personal interview shall be conducted when necessary to resolve any significant information and/or inconsistencies developed during the investigation. In departments or agencies with policies sanctioning the use of polygraph for personnel security purposes, the personal interview may include a polygraph examination, conducted by a qualified polygraph **examiner**;

e. **Birth.** Independent certification of date and place of birth received directly from appropriate registration authority if not otherwise verified under f., below, or if a variance is developed.

f. **Citizenship.** Subject must be a U.S. citizen. Independent verification of citizenship received directly from appropriate registration authority. For foreign-born immediate family members 18 years of age or older, verification of citizenship or legal status is also required. Subject's citizenship status must be verified in **all** cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally such documentation should be presented to the DoD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DoD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native-born U.S. citizens except as indicated in **4.e.** above. In the case of foreign-born U.S. citizens, DIS will check **I&NS** records. The citizenship status of all **foreign-bom** members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel **security** determination purposes:

(1) A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be certified with the registrar's signature and the raised, impressed, or multicolored seal of his office except for states or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

(a) A delayed birth certificate (a record filed more than one year after the date of birth) is acceptable provided that it shows that the report of birth was supported by acceptable secondary evidence of birth as described in subparagraph (b), below.

(b) If such primary evidence is not obtainable, a notice from the registrar stating that no birth record exists should be submitted. The notice shall be accompanied by the best combination of secondary evidence obtainable. Such evidence may include a baptismal certificate, a certificate of circumcision, a hospital birth record, affidavits of persons having personal knowledge of the facts of the birth, or other documentary evidence such as early census, school, or family bible records, newspaper files and insurance papers. Secondary evidence should have been created as close to the time of birth as possible.

(c) All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

(2) A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

(3) A certificate of citizenship issued by the **I&NS** shall be submitted if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(4) A Report of Birth Abroad of A Citizen of The United States of American (Form FS-240), a Certification of Birth (Form FS-545 or **DS-1350**), or a Certificate of Citizenship is acceptable if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(5) A passport or one in which the individual was included will be accepted as proof of citizenship.

g. **Education:** Independent verification of most recent or most significant claimed attendance and/or degree/diploma within the scope of investigation via sealed transcript received directly from the institution. If all education is outside of the investigative scope, the last education above high school level will be verified.

h. **Employment:** Direct verification through records of all periods of employment within scope but in any event the most recent two (2) years. Personal interviews of two sources (supervisor/coworkers) for each employment of six months or more shall be attempted. In the event that no employment exceeds six months, interviews of supervisor/coworkers shall be attempted. All periods of unemployment in excess of sixty (60) days shall be verified through records and/or sources. All prior federal/military service and type of discharge(s) shall be verified.

(1) **Non-Federal employment.** Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part-time, and temporary employment. Interview one supervisor and one co-worker at subject's current place of employment as well as at each prior place of employment during the past 10 years of six months duration or longer. The interview requirement for supervisors and co-workers does not apply to seasonal, holiday, Christmas, part-time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

(2) **Federal employment.** All Federal employment will be verified within the period of investigation to include Christmas, seasonal temporary, summer hire, part-time, and holiday employment. Do not **verify** Federal employment through review of records if already verified by the requester. If Federal employment has not been verified by the requester, then subject's personnel file at **his/her** current place of employment will be reviewed. All previous Federal employment will be verified during this review. In the case of former Federal employees, records shall be examined at the Federal Records Center in St. Louis, Missouri. Interview one supervisor and one co-worker at all places of employment during the past 10 years if so employed for 6 months or more.

(3) **Military employment.** Military service for the last 10 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one co-worker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a co-worker at subject's prior duty stations where assigned for 6 months or more during the past 5 years shall be interviewed. Do not verify military employment through review of local records if already verified by the requester,

(4) **Unemployment.** Subject's activities during all periods of unemployment in excess of 60 consecutive days, within the period of investigation, that are not otherwise accounted for shall be determined.

(5) When an individual has resided outside the U.S. continuously for over one year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and co-worker.

i. **References:** Four required (at least three of which are developed). To the extent practical, all should have social knowledge of subject and collectively span the entire scope of the investigation. As appropriate, additional interviews may include cohabitants(s), **ex-spouses**, and relative(s). Interviews with psychological/medical personnel are to be accomplished as required to resolve issues. Three developed character references who have sufficient knowledge of subject to comment on his background, suitability, and loyalty shall be interviewed. Efforts shall be made to interview developed references whose combined association with subject covers the **full** period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. A listed character reference will be interviewed only when developed references are not available or when it is necessary to **identify** and locate additional developed character references or when it is necessary to **verify** subject's activities (e.g., unemployment).

j. **Neighborhood:** Interviews with neighbors for the last five years if residence exceeds six months. Confirmation of current residence shall be accomplished regardless of length to include review of rental records if necessary. In the event no residence exceeds six months, interview of neighbors should be undertaken at current residence. During each neighborhood investigation, interview two neighbors who can **verify** subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5-year period only when there is unfavorable information to resolve in the investigation. Neighborhood investigations are not required outside the United States and Puerto Rico.

k. **Credit:** Verification of the subject's financial status and credit habits at **all** locations where subject has resided, been employed, or attended school for six months or more for the last seven (7) years. Conduct credit bureau check in the 50 states, the District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. Financial responsibility, including unexplained affluence, will be stressed in all reference **interviews**.

l. **Local Agency Checks:** A check of appropriate police records, including state central criminal history record repositories, covering **all** locations where subject has resided, been employed, or attended school for six months or more during the scope of investigation, to include current residence regardless of duration. In the event that no residence, employment, or education exceeds six months, **local** agency checks should be conducted at the current residence, current employment, and last educational institution attended.

m. **Foreign Travel**. If subject has been employed, educated, traveled or resided outside of the U.S. for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph 1.f. of this Appendix. In addition, the following requirements apply:

(1) Foreign travel not under the auspices of the U.S. Government. When employment, education, or residence has occurred overseas for more than 90 days during the past 10 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State and other appropriate agencies. Efforts shall be made to develop sources, generally in the U. S., who knew the individual overseas to cover significant employment education, or residence and to determine whether the individual has worked or lived outside of the U.S. continuously for over one year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

(2) Foreign travel under the auspices of the U.S. government. When employment, education, or residence has occurred overseas for a period of more than one year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State and other appropriate agencies. Efforts shall be made to develop sources (generally in the U. S.) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

n. **Foreign Connections**. All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the U.S. or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections of the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the U.S.

o. **Organizations**. Efforts will be made during reference interviews and record reviews to determine if subject and/or **the** immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in paragraphs 2-200 a. through d. of this Regulation.

p. **Military Service**. All military service and types of discharge during the last 10 years shall be verified.

q. **Medical Records**. Medical records shall not be reviewed unless:

(1) The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

(2) The requester indicates that unfavorable information is contained in subject's medical records, or

(3) The subject lists one or more of the following on the PSQ:

(a) A history of mental or nervous disorders.

(b) That subject is now or has been addicted to the use of habit-forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

r. **Public Records**: Verification of divorce(s), bankruptcy, etc., and any other court (civil or criminal) actions to which subject has been or is a party within the scope of investigation, when known or developed. Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

s. **Ex-spouse Interview**. If the subject of investigation is divorced, the **ex-spouse** will be interviewed when the date of final divorce action is within the scope of investigation.

t. **Polygraph**: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

u. **Select Scoping**. When the facts of the case **warrant**, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

v. **Transferability**: Investigations satisfying the scope and standards specified above are transferable between agencies and shall be deemed to meet the investigative standards for access to Collateral TOP SECRET/National Security Information and Sensitive **Compartmented** Information. No **further** investigation or reinvestigation prior to **revalidation** every five years will be undertaken **unless** the agency has substantial information indicating that the transferring individual may not **satisfy** eligibility standards for clearance or the agency head determines in writing that to accept the investigation would not be in the national security interest of the United States.

w. **Updating a Previous Investigation to SSBI Standards**. If a previous investigation does not substantially meet the minimum standards of an SSBI or if it is more than 5 years old, a current investigation is required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an **SSBI**. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

3. **Periodic Reinvestigation (PR)**

a. Each DoD military, civilian, consultant, and contractor employee occupying a critical sensitive position or possessing a TOP SECRET clearance, or occupying a special access program position and **non-U.S.** citizens (foreign nationals and/or immigrant aliens) holding a limited access authorization **shall** be the subject of a PR initiated 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

b. **Minimum Investigative Requirements**. A PR shall include the following minimum scope.

(1) **NAC**. A valid NAC on the SUBJECT will be conducted in all cases (NOTE: only a name check of the FBI/ID will be conducted unless records indicate that a technical fingerprint check was not done previously). Checks of **DCII, FBI/HQ**, FBI/ID name check only, and other agencies deemed appropriate, will be conducted on the Subject's current spouse or cohabitant if not previously conducted. Additionally, NACS will be conducted on immediate family members, 18 years of age or older, who are **non-U.S.** citizens, if not previously accomplished.

(2) **Credit**. Credit bureau checks covering all places where the SUBJECT resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 states, District of Columbia, Puerto Rico and overseas (where **APO/FPO** addresses are provided), will be conducted.

(3) **Subject Interview**. **The** interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, should not be explored again unless additional relevant information warrants **further** coverage.

(4) **Employment**. Current employment will be verified. Military **and** federal service records will not routinely be checked, if previously checked by the requester when the PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted. Records need be checked only when they are locally available, unless unfavorable information had been detected.

(5) **Employment References**. Two supervisors or co-workers at the most recent place of employment or duty station of 6 months; if the current employment is less than 6 months employment reference interviews will be conducted at the next prior place of employment, which was at least a 6-month duration.

(6) **Developed Character References (DCRs)**. Two developed character references who are knowledgeable of the SUBJECT will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

(7) **Local Agency Checks (LACs)**. DIS will conduct local agency checks on the SUBJECT at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations (except overseas locations from which military members have transferred).

(8) **Neighborhood Investigation**. Conduct a neighborhood investigation to verify subject's current residence in the United States. Two neighbors who can verify subject's period of residence in that area and who are sufficiently acquainted to comment on the subject's suitability for a position of trust **will** be interviewed. Neighborhood investigations **will** be expanded beyond the current residence when unfavorable information arises.

(9) **Ex-spouse Interview**. If the subject of investigation is divorced, the **ex-spouse** will be interviewed when the date of final divorce action is within the period of investigation.

(10) Polygraph: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

(11) Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

4. Secret Periodic Reinvestigation (S-PR)

a. Each DoD military, civilian, consultant, and contractor employee with current access to SECRET information shall be the subject of a S-PR initiated 10 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

b. Minimum Investigative Requirements. The S-PR shall include the following minimum scope.

(1) NAC. A NAC with a name check of the FBI Identification Division, a check of the FBI Investigative Files, as well as other agencies' indices, e.g. DoD, **OPM**, CIA, State, INS, etc., as appropriate. (Note: A technical fingerprint check of the FBI Identification Division will be conducted vice a name check if one was not done previously);

(2) Credit. Conduct credit bureau checks at all locations where subject has resided, been employed, or attended an institution of higher learning for a period of six months or more during the period of coverage;

(3) The investigation may be expanded as necessary to fully develop or resolve an issue.

APPENDIX F

DOD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

A. Officials Authorized To Grant ~~Deny~~ or Revoke Personnel Security Clearances (Top Secret, Secret, and Confidential).

1. Secretary of Defense and/or single designee
2. Secretary of the Army **and/or** single designee¹
3. Secretary of the Navy and/or single designee¹
4. Secretary of the Air Force and/or single designee¹
5. Chairman of the Joint Chiefs of Staff **and/or** single designee
6. Director, Washington Headquarters Services, and/or single designee
7. Director, National Security Agency, and/or single designee ^{1,2}
8. Director, Defense Intelligence Agency, and/or single designee ¹
9. Deputy General Counsel, Legal Counsel, OGC, and/or single designee (for contractors under the Defense Industrial Security Program (DISP))
10. Director, Defense Investigative Service, and/or single designee, (may grant security clearances only for contractor personnel under the DISP)

B. Officials Authorized To Grant ~~Deny~~ or Revoke LAA.

Officials listed in subsection A. 1 through A.10., above, and the Commanders of the Unified Combatant Commands, or their single designee, (must be **at** general officer, flag rank or civilian equivalent).

C. Officials Authorized To Certify Personnel Under Their Jurisdiction for Access to Critical Nuclear Weapon Design Information.

¹ Authority to grant, deny or revoke **access** to SCI is a **function** of the Senior Officials of the Intelligence Community (SOIC), or their designated representative, as identified in E.O. 12333 and Director of Central Intelligence Directive (DCID) 1/14. The authority for making SCI access determinations may also be the same **official** making **security** clearance determinations.

² Reference to the Director, NSA or single designee is not intended to infringe upon the authorities or responsibilities contained in DoD Directive 5210.45, “**Personnel** Security in the National Security Agency.”

See enclosure to DoD Directive 5210.2 (reference (z)).

D. ~~Official~~ Authorized To Approve Personnel for Assignment To Presidential Support Activities.

The Executive Secretary to the Secretary of Defense and the Deputy Secretary of Defense, or designee.

E. Officials Authorized To Grant Access To S1OP-ESI:

1. Director of Strategic Target Planning
2. Director, Joint Staff
3. Chief of **Staff**, U.S. Army
4. Chief of Naval Operations
5. Chief of Staff, U.S. Air Force
6. Commandant of the Marine Corps
7. Commanders of the Unified Combatant Commands

8. The authority may be **further** delegated in writing by the officials in subsections E. 1. through E.7. to the applicable subordinates.

F. Three member PSAB shall be formed under the auspices of the following officials to render final determinations when an unfavorable personnel security determination is appealed under paragraph 8-201 .d. of the Regulation.

1. Secretary of the Army
2. Secretary of the Air Force
3. **Secretary** of the Navy
4. Chairman of the Joint Chiefs of Staff
5. Director, NSA
6. Director, DIA
7. Director, **WHS**
8. General Counsel, DoD (contractors only)

G. Officials Authorized To Suspend Access to classified information:

1. Security Clearances.

a. Contractor Personnel. The Director, Counterintelligence and Security Programs; ODASD (I&S); OASD(C3I) and the Deputy General Counsel (**Legal** Counsel), **Office** of General Counsel, OSD

b. Military and/or Civilian Personnel. Commander and/or Agency head, head of the **Component**, or adjudicative authority.

2. SCI.

Cognizant **SOICs**, or their designees.

H. Officials Authorized To Issue Interim Clearances.

1. Interim TOP SECRET clearances may be issued by the officials listed in section A., above. That may be **further** delegated on determination by the head of the Agency.

2. Interim SECRET and/or CONFIDENTIAL clearances may be issued by the officials listed in section A., above, as well as by organizational commanders.

I. Officials Authorized To Designate Nonappropriated Fund Positions of Trust:

The Heads of the DoD Components, or their designees.

APPENDIX I

Adjudicative Guidelines for Determining Eligibility for Access to Classified **Information**

PURPOSE

The following adjudicative guidelines are established for **all** U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified **information**, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in **all** final clearance determinations.

ADJUDICATIVE PROCESS

The adjudicative process is an **examination** of a **sufficient** period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the **careful** weighing of a number of variables known as the whole person concept. All available, reliable information about the **person**, past and present, favorable and **unfavorable, should** be considered in reaching a determination. In evaluating the relevance of an individual's **conduct**, the adjudicator should consider the following **factors**:

The nature, extent, and seriousness of the conduct

The circumstances surrounding the conduct, to include knowledgeable participation

The frequency and recency of the conduct

The individual's age and maturity at the time of the conduct

The voluntariness of participation

The presence or absence of rehabilitation and other pertinent behavioral changes

The motivation for the conduct

The potential for pressure, coercion, exploitation, or duress

The likelihood of continuation or recurrence

Each case must be judged on its own merits and **final** determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following:

- A. Allegiance to the United States
- B. Foreign influence
- C. Foreign preference
- D. Sexual behavior
- E. Personal conduct
- F. Financial considerations
- G. Alcohol consumption
- H. Drug involvement
- I. Emotional, mental, and personality disorders
- J. Criminal conduct
- K. Security violations
- L. Outside activities
- M. Misuse of Information Technology Systems

Each of the foregoing should be evaluated in the context of the whole person.

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available **information** reflects a recent or recurring pattern of questionable **judgment**, irresponsibility, or emotionally unstable behavior.

However, notwithstanding the whole person **concept**, pursuit of **further** investigation maybe terminated by an appropriate adjudicative agency in the **face** of reliable, significant, disqualifying, adverse **information**.

When information of security concern becomes known about **an** individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

- (1) voluntarily reported the **information**;
- (2) sought assistance and followed professional guidance, where appropriate;
- (3) resolved or appears likely to favorably resolve the security concern;

- (4) has demonstrated positive changes in behavior and **employment**;
- (5) should have his or her access temporarily suspended pending final adjudication of the information.

If after evaluating information of security **concern**, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it maybe appropriate to recommend approval with a warning that **future** incidents of a similar nature may result in revocation of access.

The **information** in bold print at the beginning of each adjudicative guideline provides a brief explanation of its relevance in **determining** whether it is clearly consistent with the interest of national security to grantor continue a person's eligibility for access to classified information.

ADJUDICATIVE GUIDELINES

ALLEGIANCE TO THE UNITED STATES

An individual must be of unquestioned allegiance to the United States. The **willingness** to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) involvement in any act of sabotage, espionage, **treason, terrorism**, sedition, or ~~other~~ act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;
- (2) association or sympathy with persons who are attempting to **commit**, or who are committing, any of the above acts;
- (3) association or sympathy with persons or organizations that advocate the overthrow of the United States **Government**, or any state or **subdivision**, by force or violence or by other unconstitutional means;
- (4) involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others **from** exercising their rights under the **Constitution** or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

- (1) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
- (2) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;
- (3) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;
- (4) the person has had no recent proscribed involvement or association with such activities.

FOREIGN INFLUENCE

A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by **affection**, influence, or obligation are: (1) not citizens of the United States or (2) maybe subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) an immediate family member, or a person to whom the individual has close ties of affection or **obligation**, is a citizen **of**, or resident or present in, a foreign country;
- (2) sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
- (3) relatives, cohabitants, or associates who are connected with any foreign government;
- (4) failing to report, where **required**, associations with foreign nationals;
- (5) unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
- (6) conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign **government**;
- (7) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;
- (8) a substantial **financial** interest in a country, or in any foreign owned or operated business that could make the **individual** vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

- (1) a determination that the immediate **family** member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk;
- (2) contacts with foreign citizens are the result of official U.S. Government business;
- (3) contact and correspondence with foreign citizens are casual and infrequent;
- (4) the individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;
- (5) foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

FOREIGN PREFERENCE

When an individual acts in such away as to indicate a preference for a foreign country over the United States, then he or she maybe prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) the exercise of dual citizenship;
- (2) possession and/or use of a foreign passport;
- (3) military service or a willingness to bear arms for a foreign country;
- (4) accepting educational, medical, or other benefits, such as retirement and social **welfare**, **from** a foreign country;
- (5) residence in a foreign country to meet citizenship requirements;
- (6) using foreign citizenship to protect financial or business interests **in** another country;
- (7) seeking or holding political office in the foreign country;
- (8) voting in foreign elections; and
- (9) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

- (1) dual citizenship is based solely on parents' citizenship or birth **in** a foreign country;
- (2) indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
- (3) activity is sanctioned by the United States;
- (4) individual has expressed a willingness to renounce dual citizenship.

SEXUAL BEHAVIOR

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, **subjects** the individual to undue influence or coercion, or reflects lack of judgment or discretion.¹ (Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance)

Conditions that could raise a security concern and maybe disqualifying include:

- (1) sexual behavior of a criminal nature, whether or not the individual has been **prosecuted**;
- (2) compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
- (3) sexual behavior that causes an individual to be vulnerable to undue influence or coercion;
- (4) sexual behavior of a public nature and/or **that** which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

- (1) the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
- (2) the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
- (3) there is no other evidence of questionable judgment, irresponsibility, or emotional instability;
- (4) the behavior no longer serves as a basis for undue influence or coercion.

¹ The adjudicator should also consider guidelines pertaining to criminal conduct (criterion J); or emotional, mental, and personality disorders (criterion I), in determining how to resolve the security concerns raised by sexual behavior.

PERSONAL CONDUCT

Conduct involving questionable **judgment**, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The following will normally result in an unfavorable clearance action or administrative termination of **further** processing for clearance eligibility:

- (1) **refusal** to undergo or cooperate with required security processing, including medical and psychological testing; or
- (2) **refusal** to complete required security forms, releases, or provide **full, frank** and **truthful** answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and maybe disqualifying also include:

- (1) reliable, unfavorable **information** provided by associates, employers, coworkers, neighbors, and other acquaintances;
- (2) the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history **statement**, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
- (3) deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness **determination**;
- (4) **personal** conductor concealment of information that increases an individual's **vulnerability** to **coercion**, exploitation or pressure;
- (5) a pattern of dishonesty or rule violations²;
- (6) association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

- (1) the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;
- (2) the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;
- (3) the individual made prompt, good-faith efforts to correct the **falsification** before being **confronted** with the facts;

²To include violation of any written or recorded agreement made between the individual and the agency.

- (4) omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted **information** was promptly and **fully provided**;
- (5) the individual has taken positive steps to significantly reduce or eliminate vulnerability to **coercion**, exploitation, or pressure;
- (6) a refusal to cooperate was based on advice **from** legal counsel or other officials that the individual was not required to comply with security processing requirements **and**, upon being made aware of the requirement, fully and **truthfully** provided the requested information,
- (7) association with persons involved in criminal activities has ceased.

FINANCIAL CONSIDERATIONS

An individual who is financially overextended is at risk of having to engage in illegal acts to generate **funds**. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) a history of not meeting financial obligations;
- (2) deceptive or illegal financial practices such as embezzlement, employee **theft**, check **fraud**, income tax evasion, expense account fraud, **filing** deceptive loan statements, and other intentional financial breaches of **trust**;
- (3) inability or unwillingness to satisfy debts;
- (4) unexplained affluence;
- (5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

- (1) the behavior was not recent;
- (2) it was an isolated **incident**;
- (3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of **employment**, a business **downturn**, unexpected medical emergency, or a death, divorce or separation);
- (4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
- (5) the **affluence** resulted from a legal source; and
- (6) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

ALCOHOL CONSUMPTION

Excessive alcohol consumption **often** leads to the exercise of questionable **judgment**, unreliability, failure to control impulses, and increases the risk **of** unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and maybe disqualifying include:

- (1) alcohol-related incidents away from **work**, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
- (2) alcohol-related incidents at **work**, such as reporting for work or duty in **an** intoxicated or impaired condition, or drinking on the job;
- (3) diagnosis by a **credentialed** medical professional³ of alcohol abuse or alcohol dependence;
- (4) habitual or binge consumption of alcohol to the point of impaired **judgment**;
- (5) consumption of **alcohol**, subsequent to a diagnosis of alcoholism by a **credentialed** medical professional³ and following completion of an alcohol rehabilitation program

Conditions that could mitigate security concerns include:

- (1) the alcohol related incidents do not indicate a pattern,
- (2) the problem occurred a number of years ago and there is no indication of a recent problem
- (3) positive changes in behavior **supportive** of sobriety;
- (4) following diagnosis of alcohol abuse or alcohol dependence, the individual has **successfully** completed inpatient or outpatient rehabilitation along with **aftercare** requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 312 months, and received a favorable prognosis by a credentialed medical professional.

³ **credentialed** medical professional: licensed physician, licensed clinical psychologist, or board certified psychiatrist

DRUG INVOLVEMENT

Improper or illegal involvement with drugs, raises questions regarding an individual's willingness or ability to protect classified **information**. Drug abuse or dependence may impair social or occupational **functioning**, increasing the risk of an unauthorized disclosure of classified **information**.

Drugs are defined as mood and behavior altering:

- (a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and **hallucinogens**) and
- (b) inhalants and other similar substances.

Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and maybe disqualifying include:

- (1) any drug abuse (see above **definition**);
- (2) illegal drug possession including cultivation processing, manufacture, purchase, sale, or **distribution**;
- (3) failure to **successfully** complete a drug treatment program prescribed by a **credentialed** medical professional Current drug involvement especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

Conditions that could mitigate security concerns include:

- (1) the drug involvement was not **recent**;
- (2) the drug involvement was an isolated or infrequent **event**;
- (3) a demonstrated intent not to abuse any drugs in the future;
- (4) satisfactory **completion** of a drug treatment program prescribed by a **credentialed** medical professional.

³ **credentialed** medical professional: licensed physician, licensed clinical psychologist, or board certified psychiatrist

EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS

Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in **judgment**, reliability or stability.

When appropriate, a credentialed mental health **professional**,⁴ acceptable to or approved by the **government**, should be consulted so that potentially **disqualifying** and mitigating **information** may be **fully** and properly evaluated.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) a diagnosis by a credentialed mental health professional that the individual has a disorder that could result in a defect in psychological, social, or occupational **functioning**;
- (2) information that suggests that an individual has **failed** to follow appropriate medical advice relating to treatment of a diagnosed disorder, e.g. failure to take prescribed medication,
- (3) a pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;
- (4) information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

- (1) there is no indication of a current problem;
- (2) recent diagnosis by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or **exacerbation**;
- (3) the past emotional instability was a temporary condition (e.g., one caused by a **death**, illness, or marital breakup), the situation has been **resolved**, and the individual is no longer emotionally unstable.

⁴ credentialed mental health professional: licensed clinical psychologist, licensed social worker, or board certified psychiatrist

CRIMINAL CONDUCT

A history or pattern of criminal activity creates doubt about a person's **judgment**, reliability and trustworthiness.

Conditions that could raise a security concern and maybe disqualifying include:

- (1) any criminal **conduct**, regardless of whether the person was formally **charged**;
- (2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

- (1) the criminal behavior was not **recent**;
- (2) the crime was an isolated incident;
- (3) the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;
- (4) the person did not voluntarily commit the act and/or the factors leading to the violation are not likely to **recur**;
- (5) there is clear evidence of **successful** rehabilitation.

SECURITY VIOLATIONS

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and maybe disqualifying include:

- (1) unauthorized disclosure of classified **information**;
- (2) violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

- (1) were **inadvertent**;
- (2) were isolated or **infrequent**;
- (3) were due to improper or inadequate training;
- (4) demonstrate a positive attitude towards the discharge of security responsibilities.

OUTSIDE ACTIVITIES

Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and maybe **disqualifying** include:

Any service, whether compensated, volunteer, or employment with:

- (1) a foreign country;
- (2) any foreign national;
- (3) a representative of any foreign interest;
- (4) any foreign, domestic, or international organization or person engaged in analysis, **discussion**, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

- (1) evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;
- (2) the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

Noncompliance with rules, procedures, guidelines or regulations **pertaining** to **information** technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Information Technology Systems include all related equipment used for the communication, **transmission**, processing, **manipulation**, and storage of classified or sensitive information.

Conditions that could raise a security concern and maybe **disqualifying** include:

- (1) Illegal or unauthorized entry into any information technology system,
- (2) Illegal or unauthorized modification, destruction, manipulation, or denial of access to **information** residing on an information technology system;
- (3) Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
- (4) Introduction of hardware, **software** or media into any information technology system without **authorization**, when specifically prohibited by rules, procedures, guidelines or regulations;

Conditions that could mitigate security concerns include:

- (1) The misuse was not recent or significant;
- (2) The conduct was unintentional or inadvertent;
- (3) The introduction or removal of media was authorized;
- (4) The misuse was an isolated event;
- (5) The misuse was followed immediately by a **prompt**, good faith effort to correct the situation.

APPENDIX L

LIST OF SAMPLE NOTIFICATIONS

Initial Package to Notify Organization and Individual

Local Organization Letter with SOR	L-2
Sample SOR (Enclosure 1 to Letter)	L-4
Security Concerns and Supporting Adverse Information	L-5
Instructions for Responding to SOR	L-6
Sample Applicable Personel Security Guidelines (Enclosure 2 to Letter)	L-8
SOR Receipt and Statement of Intention (Enclosure 3 to Letter)	L-9
Form Requesting Personnel Security Investigation	L-10

Package to Inform Organization and Individual of Denial

Local Organization Letter with LOD	L-11
Sample Letter of Denial (Enclosure to Letter)	L-12
Notice of Intent to Appeal	L-14
Instructions for Appealing a Letter of Denial/Revocation (LOD)	L-15

Local Organization Letter with Statement of Reasons (SOR)

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphics Facility, Washington, DC

Subject: RESPONSIBILITY FOR HANDLING STATEMENT OF REASONS (SOR)

Reference: (a) (Component Personnel Security Regulation)

Enclosure: 1. SOR
2. SOR Receipt and Statement of Intention
3. Form for Requesting (**Personnel** Security Investigation)

1. The purpose of this letter is to provide instructions for actions required by your organization related to the individual named in the enclosed SOR. Since denial or revocation of access eligibility can have a severe impact on individuals and their careers, procedures required by **reference** (a) must be closely followed to ensure that both security and fairness requirements are met.

2. Your organization is responsible for completing the following actions with regard to the individual named in the SOR

a. Consider whether or not to suspend access to classified information and assignment of the individual to nonsensitive duties pending a final personnel security decision. Failure to do so could result in an increased level of security risk.

b. Designate a person from your **organization** as the point of contact (**POC**) in this matter pursuant to paragraph 8-201(a), reference (a), above. This person will serve as a liaison between the (Component) Central Adjudication Facility (**CAF**) and the individual.

3. The POC from your organization should:

a. Promptly deliver enclosure (1) to this letter, the SOR and its enclosures, to the named individual.

b. Complete and forward enclosure (2) to this letter to the **CAF** within 10 calendar days. Ensure that Parts I, II, and III are all completed. This form notifies the **CAF** whether the individual intends to respond to the SOR and whether your organization has granted a time extension.

c. Advise the individual that he or she should not attempt to communicate directly with the **CAF** except in writing, and that, if necessary, he or she should seek the assistance of your organization's designated POC. Also, ensure that the individual understands that he or she is entitled to obtain legal counsel or other assistance but that this must be done at the individual's own expense.

d. Ensure that the individual understands the consequences of being found ineligible for access to classified information and performance of sensitive duties **and** the serious effect such a determination could have on his or her career.

e. Take particular care to ensure that the individual **fully** understands that the proposed denial or revocation action will become final if your organization notifies the **CAF** via enclosure (2) that the individual does not intend to respond to the SOR. Ensure that the individual understands that failure to submit a timely reply will result in **forfeiture** of any **further** opportunity to contest this unfavorable personnel security determination

f. Explain procedures for requesting a time extension for responding to the SOR. If the individual requires additional time to obtain copies of investigative records and/or to prepare his or her response, your organization may grant an extension of up to 30 additional calendar days. The **CAF** must be notified of such an extension using enclosure (2). See **reference** (a) for more detail.

g. Assist the individual in obtaining applicable references and copies of pertinent investigative files. The SOR is usually based on investigative information from the Defense Investigative Service (**DIS**) and/or another investigative agency. If the individual desires copies of releasable **information** pertinent to this **SOR**, a request may be submitted to the **CAF** using the receipt at enclosure (2). If the individual wants to obtain a copy of the complete investigative file, provide him or her with enclosure (3) which is the form for requesting [**DIS** and/or other investigative agency] records under the Privacy Act (5 U.S.C. 552a.).

4. Ensure that the individual's response to the SOR is promptly endorsed by appropriate authority and immediately forwarded to the **CAF**. Submissions to the CAF are deemed to have been made when actually received by the CAF, or **postmarked**, whichever is sooner. This endorsement should include observations and comments regarding the person's **judgment**, reliability **and** trustworthiness as well as a recommendation regarding the decision at hand. An endorsement that does not include comments and a recommendation will be taken to mean that your **organization** concurs with the unfavorable personnel security determination.

5. (Additional component-specific requirements)

6. If you have any questions, the point of contact at the CAF is Mr. John Doe, DSN 000-0000 or commercial (000) 000-0000, e-mail **doejohn@caf.dod**.

Statement of Reasons (SOR)

From: Director, [Component] Central Adjudication Facility
Through: Director, Service Graphics Facility, Washington DC
To: Mr. John Doe, SSN 000-00-0000

Subject: INTENT TO (DENY/REVOKE) ELIGIBILITY FOR ACCESS TO CLASSIFIED
INFORMATION OR ASSIGNMENT IN SENSITIVE DUTIES

Reference: (a) Component Personnel Security Regulation

Enclosure: 1. Security Concerns and Supporting Adverse Information
2. Instructions for **Responding** to a Statement of Reasons
3. Applicable **Personnel** Security Guidelines

1. A preliminary decision has been made to (deny/revoke) your eligibility for access to classified **information** or employment insensitive duties. Adverse **information** from an investigation of your personal history has led to the security concerns listed in enclosure (1) and has raised questions about your trustworthiness, reliability, and judgment. If this preliminary decision becomes final, you will not be eligible for access to classified information or employment in sensitive duties as defined by reference (a).

2. You may challenge this preliminary decision by responding, in writing, with any information or explanation which you think should be considered in reaching a final decision. Enclosure (2) is provided to assist you if you choose to respond. Enclosure (3) provides an extract from reference (a) of the specific personnel security guidelines used in the **preliminary** decision to (deny/revoke) your eligibility for access to classified **information** employment in sensitive duties. The **preliminary** decision will become **final** if you **fail** to respond to this letter. You may obtain legal counsel or other assistance; however, you must do so at your own expense.

3. You must **notify** your (Component) Central Adjudication Facility (CAP) via the head of your organization within 10 calendar days as to whether or not you intend to respond. If you choose not to **respond**, you will forfeit an opportunity to contest this unfavorable personnel security determination. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days from the date you received this letter. Your organization may grant up to 30 additional calendar days if you submit a written request to your security **office**. Additional time extensions may only be granted by the **CAF**. Contact the point of contact with the CAP for help in preparing and forwarding your notice of an intent to respond and your response and if you wish to obtain releasable investigative records used in your case.

4. **If** you currently have access to classified information, this access (is/may be) suspended pending the final decision. Please direct questions regarding this letter to your security officer or the point of contact with the **CAF**.

Security Concerns and Supporting Adverse Information

Subject of Investigation (Mr. John Doe, 000-00-0000)

Statement of Reasons

1. Available information tends to show criminal or dishonest conduct on your part

- a. You were arrested on 28 March 1985 in Arlington, VA, for assault on a police officer. You were found **guilty** and fined \$4,000.
- b. You were **arrested** on 10 **January** 1993 in **Fairfax**, VA, and charged with **interfering** with an **arrest**. You were released on \$300 bail which you forfeited for **failure** to appear.
- c. You were arrested on 22 June 1994 in Fairfax, VA, on a bench warrant and charged with **failure** to appear (as set forth above). You were found guilty of **interfering** with an arrest on 10 January 1993 (as set forth above) and fined \$400. The charge of failure to appear was dismissed.

2. Available information tends to show financial irresponsibility on your part

- a. You filed for Bankruptcy under Chapter 7 in the U.S. District **Court**, Washington DC on 10 August 1987. You were discharged from debts
- b. A judgment was entered against you for \$2,500 on 20 July 1992, in the Superior **Court**, Washington, DC. As of 30 January 1995, the judgment had not been paid.
- c. As of 20 July 1994, your credit account with the Hecht Company, **Washington**, DC was \$350 overdue and referred for collection.
- d. As of 20 July 1994, your credit account with J.C. Penney Co., Arlington, VA, was \$500 overdue and referred for collection.

Instructions for Responding to a Statement of Reasons (SOR)

A **preliminary** decision has been made to deny or revoke your eligibility for access to classified information or employment in sensitive duties. This preliminary decision will automatically become final if you fail to **notify** the Central Adjudication Facility (CAF) within 10 days that you intend to respond to the SOR. You will also lose your right to appeal that final decision if you do not submit a timely response. If this decision becomes final, you will not be eligible to handle classified information or **perform** sensitive duties. This could prevent you from continuing in your present position or pursuing your **current** career.

The SOR is based on adverse **information** revealed by an investigation into your personal history. Specific security concerns about your conduct or **background**, along with supporting adverse **information**, are listed in enclosure (1) to the Statement of Reasons.

These instructions are intended to help you provide the most accurate and relevant information as to why the preliminary decision should be overturned. However, it is only a guide. You should provide whatever information you think ought to be considered in reaching the final decision.

It is in your best interest to provide the most complete and accurate **information** possible at this stage in the decision-making process. Therefore, if you decide to challenge the preliminary decision, you must respond to the statement of reasons as completely as possible.

A. Before Responding

(1) Follow the instructions. The SOR and these instructions provide specific requirements and deadlines for compliance. You will forfeit your right to appeal if you fail to follow these instructions. You must **notify** the CAF via the point of contact (POC) within 10 calendar days as to whether or not you intend to respond. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days **from** the date you received the SOR, unless you requested and were granted an extension of time.

(2) Review adverse information. You should **carefully** read the security concerns and supporting adverse information (enclosure 1) to the SOR to determine if the findings are accurate and whether there are circumstances that were not included and which might have a favorable bearing in your case. You may obtain relevant investigative or other information pertinent to the adverse **information** listed in enclosure (1) to the SOR. In **addition**, you may obtain a complete copy of releasable investigative records concerning your personal history under the provisions of the Privacy Act. Your security officer or point of contact with the CAF can help you obtain copies of these records. If you do submit a request for your investigative records, make sure to ask the POC for a time extension to the deadline for responding to the SOR since it may take up to 30 calendar days to receive these records.

(3) **Obtain** and organize supporting documents. Gather any documentation that supports your case. Documentation should be organized according to the security concerns presented in enclosure (1). The most **useful** documents will be those that **refute**, correct, explain, extenuate,

f
....
mitigate, or update the adverse information presented in enclosure (1). Examples of useful documentation include copies of correspondence; court records with details or dispositions of **arrests** and status of probation, **receipts**; copies of canceled checks or letter from creditors verifying the status of delinquent accounts; certificates of completion for rehabilitation programs; releases from judgment or **attachment**; transcripts of court testimony taken under **oath**; probation **reports**; copies of negotiated plea bargains; etc. Mere statements, such as "I paid those bills," "I didn't do **it**," or "It wasn't my **fault**," will not carry as much weight **as** supporting documentation. You may provide statements **from** co-workers, supervisors, your commander, friends, neighbors and others concerning your **judgment**, reliability and trustworthiness, and any other **information** that you think ought to be considered before a final decision is made.

(4). Seek assistance. An individual at your organization has been designated as a point of contact with the CAF on this matter. If this person cannot answer your questions, he or she can request assistance from higher authority. The process is designed so that individuals can represent themselves. Nonetheless, you may obtain legal counsel or other assistance in preparing your response. However, if you obtain assistance, it must beat your own expense.

Remember -- it is up to you to decide whether to respond. You are responsible for the substance of your response and it must be signed by you.

B. Writing a Response

(1) Your response should be in the form of a letter from you to the **CAF**. You should address each security concern separately. You should admit or deny each security concern and admit or deny each item of supporting adverse **information**.

(2) It is essential that you address each security concern and the adverse information cited to support it. Provide any **information** that explains, refutes, corrects, extenuates, mitigates or updates each security concern. Include, wherever possible, copies of the types of documents described above. Organize supporting documents in the order that they are referred to in your letter and enclose copies with your letter. Finally, be sure to sign and date your letter.

(3) The impact of your response will depend on the extent to which you can specifically **refute, correct**, extenuate, mitigate, or update security concerns and adverse information presented in enclosure (1). Information that is untrue should be specifically **refuted**. If you believe that the adverse **information**, though true, does not support the security concern or presents an incomplete picture, you should provide **information** that explains your case. This additional information could help you disprove or lessen the security concern.

(4) Personnel security guidelines are used by decision-makers to determine whether certain adverse information is of security concern. The guidelines pertinent to security concerns **in** your case are listed in enclosure (3) to the SOR. These guidelines are general rules used by **decision-makers** in determining whether an individual should be granted eligibility for access to classified **information** or permitted to perform sensitive duties. The guidelines provide a framework for weighing all available information, both favorable **information** as well as adverse information

that is of security concern. The guidelines help decision-makers make a common-sense determination concerning an individual's eligibility for access to classified information and **performance** of sensitive duties based upon all that is **known** about an individual's personal history.

(5) Place your written response and supporting documents in a single envelope or package and forward it to the CAP via the head of your organization. Your organization will add its comments at that time. An endorsement by your organization that does not include substantive comments and a recommendation will be interpreted to mean that your **organization** concurs with the SOR. Be sure to meet the time deadlines. You will be notified in writing of the **final** decision. Inmost cases this decision will be made within 60 days. If the decision is in your favor, your access eligibility will be granted or restored. If not, you may appeal the decision to a higher authority.

Applicable Personnel Security Guidelines

The relevant personnel security guidelines are listed below for each area of security concern in your case. The security concerns and supporting adverse **information** are provided in enclosure (1).

Security Concern: Available information tends to show criminal conduct on your part.

A history or pattern of criminal activity creates doubt about a person's **judgment**, reliability and trustworthiness. Conditions that signal security concern and may be **disqualifying** include: (1) any criminal **conduct**, regardless of whether the person was formally charged; (2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include: (1) the criminal behavior was not **recent**; (2) the crime was an isolated **incident**; (3) the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life; (4) the person did not intentionally commit the act and the factors leading to the unintentional violation are not likely to **recur**; (5) there is clear evidence of **successful** rehabilitation.

Security Concerⁿ Available information tends to show financial irresponsibility or unexplained affluence on your part.

An individual who is financially overextended is at greater risk of having to choose between significantly reducing lifestyle or engaging in illegal acts to generate **funds**. Unexplained **affluence** is often linked to proceeds from financially profitable criminal acts. Conditions that signal security concern and may be disqualifying include: (1) a history of not meeting financial obligations resulting in bankruptcy; (2) deceptive or illegal financial practices such as **embezzlement**, employee **theft**, check fraud, income tax evasion, expense account **fraud**, filing deceptive loan statements, and other intentional financial breaches of **trust**; (3) being unable to **satisfy** debts **incurred** to creditors; (4) unexplained affluence; (5) **financial** problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include: (1) the behavior was not recent; (2) it was an isolated incident; (3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment a business downturn, unexpected medical emergency, or a **death**, divorce or separation); (4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control; (5) the affluence resulted **from** a legal source; and (6) the individual initiated a **good-faith** effort to repay overdue creditors.

SOR Receipt and Statement of Intention

From: Director, Service Graphics Facility
To: Director, (Component) Central Adjudication Facility
Subject Acknowledgment of Receipt for Statement of Reasons

1. I acknowledge **receipt** and delivery of your Statement of Reasons (**SOR**) to Mr. John Doe, SSN 000-00-0000. Parts I, II, III and IV of this form have been completed as requested.

PART I

I have received an SOR on this date from the (Component) Central Adjudication Facility.

(Signature)

(Date)

PART II

I intend to:

- a. ☐ submit no reply to the SOR.
- b. ☐ respond to the SOR but have requested an extension for the following reasons:

- c. ☐ respond via my organization head within 30 calendar days of the date I acknowledged receipt of the SOR.

(Signature)

(Date)

PART III

Check one of the following:

- a. ☐ I request relevant copies of documents and records upon which the SOR is based;
- b. ☐ I do not desire relevant copies of documents and records upon which the SOR is based.

PART IV

This organization

- a. ☐ has not granted an extension.
- B. ☐ has granted an extension until

(Date)

Point of Contact:

(Print Name)

(Position)

Local Organization Letter with LOD

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphic Facility, **Washington**, DC

Subject: RESPONSIBILITIES FOR HANDLING LETTER OF
(DENIAL/REVOCAION)

Enclosure: 1. Letter of Denial/Revocation (**LOD**)
2. LOD Receipt

1. A decision has been made by the Central Adjudication Facility (CAP) to (deny/revoke) the (security clearance, SCI access, employment in sensitive duties) of the individual named in the enclosed LOD. The purpose of this letter is to provide instructions for actions required by your organization.

2. If not already accomplished, your organization is responsible for completing the following actions with regard to the individual named in the LOD:

- a. Terminate access to classified information and/or **assignment** to sensitive duties.
- b. Designate a person from your organization as the point of contact in this matter.

3. **Your** point of contact (**POC**) on this matter should promptly deliver enclosure (1) to the named individual. Have the individual sign and date enclosure (2) upon receipt of the LOD. This signature verifies receipt of the LOD and should be retained by your organization until the final disposition of the appeal.

4. If the subject responded to the statement of reasons, your POC should:

a. Ensure the individual understands that he has 10 calendar days, from receipt of the LOD, to submit a notice of intent to appeal and to elect whether to appeal in writing to **the** Personnel Security Appeals Board (**PSAB**) or to appear in person before a Defense Office of Hearings and Appeals (DOHA) Administrative Judge (**AJ**). He must **notify** your organization of his intended action. Any extensions to this deadline must be submitted in writing to the PSAB.

b. Ensure that the individual understands that he may elect to appeal in writing directly to the PSAB or to request a personal appearance before a DOHA AJ. If the individual desires a personal appearance, the request must be in writing. It must be sent to DOHA within 10 calendar days of the individual's receipt of the LOD. If the individual desires to appeal in writing directly to the PSAB, it must be **filed** within 30 calendar days of receipt of the LOD. A form for the notice of intent to appeal has been provided as an enclosure to the **LOD**.

5. If the subject did not respond to the statement of reasons, your POC should inform the individual the decision is final and the appeal process is concluded. Exceptions may only be granted by the CAP.
6. If your organization or the named individual has any questions, the POC should communicate with the **President**, PSAB, at DSN 000-0000 or commercial 000-00-0000, or the Director, DOHA, at Autovon 226-4598 or commercial 703-696-4598.

Letter of **Denial/Revocation**(LOD)

From: Director (Component)Central Adjudication Facility
Through: Director, Service Graphic Facility, Washington D.C.
To: Mr. John Doe, SSN 000-00-0000

Subject: FINAL (DENIAL/REVOCATION) OF ELIGIBILITY FOR ACCESS TO
CLASSIFIED
INFORMATION OR (EMPLOYMENT IN SENSITIVE DUTIES)

Reference: (a) Our **ltr** (Ser **XXX**) of (date)
(b) Personnel Security Regulation
(c) Your **ltr** of (date)

Enclosure: 1. Notice of Intent to Appeal
2. Instructions for Appealing a Letter of (Denial/Revocation)

1. Reference (a) informed you of our intent to [deny/revoke] your eligibility for access to classified information (or employment in sensitive duties). An enclosure of this reference listed security concerns and supporting adverse **information** supporting this **preliminary** decision. The contents of your response have been **carefully** considered. Our final assessment of the security concerns presented in reference (a) is as follows:

- a. Criminal conduct - The **information** you provided successfully mitigated the security concerns related to your arrest on 28 March 1985. However, you did not sufficiently address or provide any new information to explain or mitigate the other adverse information (items 1b and 1c). Your criminal conduct is still of security concern.
- b. Financial irresponsibility - While you provided an explanation for the Superior Court Judgment, you did not sufficiently address or provide any new information to explain the other adverse information (items 2a, 2c and 2d). Your financial irresponsibility is still of security concern.

2. Given the remaining security concerns, effective this date, we have (denied/revoked) your eligibility for access to classified information and for assignment to a sensitive position using the provisions of reference (b).

3. You may appeal this letter of denial (**LOD**) in one of two ways: (1) by **notifying** the Personnel Security Appeal Board (**PSAB**) within 10 calendar days **after** you receive this LOD of your **intent** to appeal directly to the PSAB and by providing the PSAB within the next 30 calendar days with any supporting material not already provided as to why the LOD should be overturned; or (2) by requesting a personal appearance before an Administrative Judge to present your case. If you request a personal appearance, it must be sent to the Director, Defense **Office** of Hearings and

Appeals (DOHA), Post Office Box 3656, **Arlington, Virginia**, 22203 (FAX No. 703-696-6865) within 10 calendar days of your receipt of the LOD. A form (enclosure 1) for requesting a personal appearance is appended. In either case, inform the head of your employing organization that you are submitting an appeal. Instructions for preparing and executing an appeal are provided at enclosure 2.

4. If you appeal, the case file including all of the information you supplied in accordance with reference (c) will be forwarded to either the **PSAB** or the DOHA for consideration. If you require **an** extension to a deadline, you must make your request in writing to the PSAB or the DOHA and **notify** the head of your organization.

5. Questions regarding this LOD should be directed to POC designated by your organization.

Use The Following If The Individual Did Not Respond To SOR:

1. Reference (a) informed you of our intent to (deny/revoke) your eligibility for access to classified information and for assignment to sensitive duties.

2. Reference (a) further informed you that the unfavorable personnel security decision would become automatically final if you failed to submit a timely response.

3. Because we have received no timely response, your eligibility for access to classified information or **performance** of sensitive duties is hereby (denied/revoked). This decision is final and is not subject to **further** appeal.

Notice of Intent to Appeal

PART I

I, (last name), (first name), (middle initial), social security number (000-00-0000),
received a Letter of **Denial/Revocation** from (Name of CAF) dated **MMDDYY**. I elect (check
one of the following):

☐ to appeal directly to PSA13

☐ a **personal** appearance before a DOHA Administrative
Judge

PART II

The following information is provided 'so that I can be contacted by the PSAB or DOHA:

a. Duty Address:

b. Duty Phone:

c. Home Address:

d. Home Phone:

PART III

This Notice must be sent to the President of the PSAB (address), or the Director, Defense
Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No.
703)-696-6865) within 10 **calendar** days from receipt of the Letter of Denial/Revocation (**LOD**).

Signature

Date

Instructions for Appealing a Letter of Denial/Revocation (LOD)

A decision has been made to deny or revoke your eligibility for access to classified information or performance of sensitive duties. This means that you are not eligible to handle classified information or perform sensitive duties. This could prevent you from continuing in your present position or pursuing your current career. The letter of denial or revocation (LOD) explains this decision. It is based on adverse information which raises security concerns about your trustworthiness, reliability or judgment.

A. How to Appeal

The LOD can be appealed in one of two ways:

1. You may request a personal appearance before an administrative judge (AJ) from the Defense Office of Hearings and Appeals (DOHA). This appearance is intended to provide you with an additional opportunity to present a full picture of your situation. You will have an opportunity to orally respond to the security concerns noted in the LOD and submit supporting documentation to the AJ who will make a recommendation to the Personnel Security Appeal Board (PSAB). The PSAB will consider both your written record and the results of the personal appearance in making its **final** decision.
2. You may, however, **prefer** to submit a written appeal to the PSAB and forego the personal appearance. If you submit a written appeal, you may also provide supporting documentation. Having or not having a personal appearance will not bias the PSAB in making a **fair** determination in your case.

You must elect either (1) or (2); you may not do both,

B. Appealing Without a Personal Appearance

If you choose to appeal without a personal appearance, your written response should provide whatever information you think ought to be considered in the **final** decision. You should try to specifically explain, **refute**, extenuate, mitigate or update **the** security concerns presented in the LOD.

You should review enclosure (2) to the **SOR**, “Instructions for Responding to a Statement of Reasons (SOR)” to make sure that your appeal follows the guidelines outlined in that document. It will help you understand how to develop and write your appeal so that it can best address the security concerns in your case. Supporting documents should be provided in the order referred to in your written response.

Place your written appeal and supporting documents in a single envelope or package and forward it to the PSAB via the head of your organization. Be sure to sign and date your appeal and submit it within 30 calendar days of your notice of appeal.

C. Appealing with a Personal Appearance

If you choose to have a personal appearance, you must provide DOHA with your request within 10 calendar days of receipt of the LOD. **You** will receive a notice designating the time, date and place for the personal ~~a~~ **appearance**, which generally will be held within 30 calendar days **after** your request. The personal appearance generally will be conducted at or near your duty station if it is in the lower 48 states. For people stationed elsewhere, it will be held at or near your duty station or at a DOHA facility in the Washington, **D.C.** or Los Angeles, California metropolitan area.

At the appearance you will have an opportunity to present oral and documentary information on your own behalf. While the personal appearance is designed so that you can represent yourself, you may obtain legal counsel or other assistance at your own expense to be present at the appearance. If you desire counsel, arrange for it now. Postponement of the personal appearance can be granted only for good cause.

In getting ready for the personal appearance, make sure that you are prepared to address all of the security concerns and supporting adverse information. **Also**, make sure that your supporting documents are organized and readily accessible for presentation to the **AJ** presiding at the appearance and for use in answering questions.

The AJ presiding at the appearance will have already reviewed your case file. Therefore, your goal should be to **clarify** your reasons for overturning the LOD and adding additional information and documentation when appropriate rather than merely to repeat material that you previously submitted. You will not have the opportunity to present or **cross-examine** witnesses. If you want the views of others presented, make sure that you obtain these views in writing (e.g., letters of reference, letters from medical authorities, etc.) and that you present these documents to the AJ.

During the appearance, you will be allowed to make an oral presentation and submit documentation. You may be asked questions. Answer clearly, completely, and honestly. The AJ is not thereto present the government's security concerns but rather to listen to any explanations that you may have concerning your case. This individual did not make the unfavorable personnel security determination set forth in the LOD, and is thereto give you an opportunity to present your case as **fully** as possible.

At the end of the personal appearance, you will be given an opportunity to make a closing statement. You should stress the highlights rather than review your entire case. Try to show how the weight of all available information supports overturning the unfavorable personnel security determination in your case.

The **AJ** will review the case file, listen to your comments and review any additional documentation that you submit, and then make a recommendation to the PSAB as to whether the clearance, access, or employment in sensitive duties should be denied, revoked or reinstated. The PSAB is not bound by the recommendation of the AJ but will consider it, as well as any additional information you present at your appearance.

APPENDIX M

STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

Component Personnel Security Appeal Boards (**PSABs**) shall be structured and function to meet the following requirements:

1. The PSAB will be comprised of three members at the minimum military grade of O-5 or civilian grade of **GM/GS-14**. In cases where the appellant is at or above the grade of military O-5 or **GM/GS-14**, at least one member of the board will be equivalent or senior in grade to the appellant.
2. One of the three members will be a permanent board member and serve as board president. This person should have a thorough knowledge of and experience in the field of personnel security.
3. One of the three members will be an attorney, unless the board has access to legal counsel, and not more than one member shall be from the security career field.
4. The composition of the board may be changed if an appellant works for a component without a **PSAB**. A senior **official** of that component will be entitled, but not required, to occupy one of the three board positions during consideration of the case.
5. Officials from the Central Adjudication Facility will neither serve as a member of the board nor communicate with board members concerning the merits of an open case.
6. Component **PSABs** will meet regularly to assure timely disposition of appeals.
7. Each case shall be reviewed by all three PSAB members. Appeals will be decided by majority vote of the board members present at a meeting to discuss and vote on the case.
8. Component PSABs will render a final determination and **notify** the individual (via the individual's local organization) in writing. The PSAB will generally **notify** individuals within 60 calendar days of the receipt of appeal (without personal appearance) or 30 calendar days of receipt of the recommendation of the Administrative Judge (if a personal appearance is requested). This written notification will provide the reasons that the PSAB either sustained or overturned the original determination of the component Central Adjudication Facility. The PSAB determination will be final and will conclude the appeal process.
9. The PSAB shall maintain a redacted file of all decisions which will be subject to review in accordance with the Freedom of Information Act.

APPENDIX N

Conduct of a Personal Appearance Before An Administrative Judge (AJ)

1. A person appealing a Letter of Denial (**LOD**) may request a personal appearance by **notifying** the Defense **Office** of Hearings and Appeals (DOHA) in writing at the following address: Director, Defense Office of Hearings and Appeals, Post Office Box 3656, **Arlington**, Virginia 22203 (FAX No. 703-696-6865). The request must be sent to DOHA within 10 calendar days of receipt of the LOD. An extension of time maybe granted by the Director, DOHA or designee for good cause demonstrated by the appellant.
2. Upon receipt of a request for a personal appearance, DOHA shall promptly request the appellant's case file from the appropriate CAF, assign the case to an AJ, and provide a copy of the request to the appropriate **PSAB**. The **CAF** shall provide the case file to DOHA normally within 10 calendar days.
3. The AJ will schedule a personal appearance generally within 30 calendar days from receipt of the request and arrange for a verbatim transcript of the proceeding. For appellants at duty stations **within** the lower 48 states, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location. For individuals assigned to duty stations outside the lower 48 states, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location, or at DOHA facilities located in the Washington, **D.C.** metropolitan area or the Los Angeles, California metropolitan area as determined by the Director, DOHA, or designee.
4. Travel costs for the appellant will be the responsibility of the employing organization.
5. The AJ will conduct the personal appearance proceeding in a fair and orderly **manner**:
 - a. The appellant may be represented by counsel or personal representative at his own expense;
 - b. The appellant may make an oral presentation and respond to questions posed by his counsel or personal representative, and shall respond to questions asked by the AJ;
 - c. The appellant may submit documents relative to whether the LOD should be overturned;
 - d. The appellant will not have the opportunity to present or cross-examine witnesses;
 - e. Upon completion of the personal appearance, the AJ will generally forward within 30 calendar days, a written recommendation to the appropriate PSAB whether to sustain or overturn the LOD, along with the case file and any documents submitted by the appellant. A copy of the AJ's recommendation will be provided to the CAF.
6. The PSAB will render a final written determination stating its rationale and **notify** the individual in writing (via the individual's employing organization) generally within 30 calendar days of receipt of the recommendation from DOHA. This decision will be final and will conclude the appeal process.